

FEDERAL PRIVACY COUNCIL

U.S. OFFICE OF PERSONNEL MANAGEMENT

<u>Toolkit for Recruiting, Hiring, and Retaining Privacy</u> <u>Professionals in the Federal Government</u>

> Version 1.0 Release: 1/13/2017

"Privacy has been at the heart of our democracy from its inception, and we need it now more than ever."

Executive Order 13719, Feb. 9, 2016.

Protecting privacy in the collection and handling of personal information is critical to the success of agency missions and to maintaining the public's trust. In order to protect privacy, each agency needs experienced and educated privacy professionals. The Federal Privacy Council was established to help agencies recruit and hire experienced privacy professionals and expand the professionals' skills and career development opportunities.

This toolkit is designed to support Federal Government efforts in understanding the multidisciplinary nature of the job of a privacy professional and the education, experience, and skills needed for such a professional. This toolkit is designed to help Federal agency human resource professionals advise organizations in the recruitment and hiring of privacy professionals, and in the career paths available to privacy professionals.

Top 10 Tips for Privacy Talent Recruiting & Hiring

1.	Ensure you have effective privacy program leadership and governance. "Our efforts to meet these new challenges and preserve our core value of privacy, while delivering better and more effective Government services for the American people, demand leadership" (E.O. 13719.) The first question for your agency is about leadership. Is the leader of your privacy program in a central leadership position at the agency? Does he or she have the necessary authority, and privacy-related skills, knowledge and experience to lead and direct the privacy program, as required by OMB? Is the program structured in ways that support its leader?	Page 25, 48 (Section II.B.5., and App. A)
2.	Privacy goes far beyond the Privacy Act. Federal agency privacy programs follow a complex variety of laws, regulations, policies and standards, and privacy professionals work at the crossroads of law, policy and technology to support diverse agency missions. Make sure that you understand the full breadth of responsibilities and make sure your staffing plan reflects the different skills you need to fulfill those responsibilities.	Page 4 (Section I.)
3.	Privacy positions are multi-disciplinary. Privacy is a robust and rapidly growing field that attracts experts from many different disciplines. Privacy positions involve responsibilities closely related to more than one discipline and can be classified in two or more occupational series, e.g., government information specialists, general attorneys, management analysts, and IT specialists.	Page 8 (Section II.B.2.)
4.	Consult OPM's Recruitment Policy Studio: https://hru.gov/Studio_Recruitment/Studio_Recruitment.aspx. Hiring Toolkit: https://hru.gov/Studio_Recruitment/HT_Hiring_Toolkit.aspx Hiring Decision Tool: https://hru.gov/Studio_Recruitment/HT_Hiring_Decision_Tool.aspx Assessment/Selection Policy: https://www.opm.gov/policy-data-oversight/assessment-and-selection/.	Page v (Introduction)
5.	Use all of the hiring authorities and flexibilities. The Presidential Management Fellows Program (PMF) now includes a privacy "discipline" to help you recruit privacy talent with advanced degrees. And also consider Peace Corps and VISTA volunteers, Scholarships for Service, Schedule A, and other hiring programs.	Page 27 (Section III.B.)
6.	Don't re-invent the wheel: Use toolkit resources. The toolkit was developed through collaboration with OPM and over 20 Federal agencies, and contains template position descriptions, job announcements, sample interview questions and more.	Pages 47-121 (Appendices)
7.	Broaden your recruiting strategy. USAJobs is a great starting point – but utilize other resources. Send your job opportunity announcement to the Federal Privacy Council listserv of more than 1000 privacy professionals across the Federal Government (see <u>www.FPC.GOV/Careers</u>); post the position in privacy groups on social media sites, and on online job boards, e.g., Monster.com.	Page 8 (Section III.B.2.)
8.	Rating and ranking: Use privacy subject matter experts! If your agency does not have any privacy subject matter experts, contact the Federal Privacy Council (FPC), <u>www.FPC.GOV/Careers</u> . The FPC may be able to find one to assist your agency.	Page 39 (Section IV.C.)
9.	Be efficient: Share certificates if you can and recruit from other agencies. Can your agency share a certificate of qualified candidates within its own agency or with another agency? Remember that current and former status Federal employees can apply to internal (MP) certificates.	Page 27 (Section III.B.)
10.	Develop your team, keep them engaged and moving up the career ladder. Train your team, let them work on cutting edge issues, and help them expand their skills and develop the competencies to move up.	Pages 47-121 (Appendices)

Acknowledgements

This toolkit has been developed by the Federal Privacy Council Workforce Committee's Talent and Career Development Subcommittee, with policy advice and guidance from the Office of Personnel Management (OPM) along with representatives from across the Federal Government, in the following agencies:

- Department of Homeland Security (DHS)
 - U.S. Immigration and Customs Enforcement
 - U.S. Citizenship and Immigration Services
 - DHS Privacy Office
- Department of Health and Human Services
 - Office of the National Coordinator for Health IT
 - o Office for Civil Rights
 - Office of the Chief Information Officer
- Department of the Interior
- Department of Defense
 - Department of the Navy
- Department of Education
- Department of Justice

- Department of Veterans Affairs
- Department of State
- Department of Treasury • Internal Revenue Service
- Department of Transportation
- Department of Housing and Urban Development
- Office of Management and Budget
- Federal Trade Commission
- Consumer Financial Protection Bureau
- Commodity Futures Trading Commission
- Federal Reserve Board
- Privacy and Civil Liberties Oversight Board
- Department of Commerce
 - National Institute of Standards and Technology

OPM and the Federal Privacy Council leadership wish to acknowledge and thank the members of the Subcommittee whose dedicated efforts contributed to this publication.

Introduction

The purpose of this toolkit is to provide assistance to Federal agency human resources staff, supervisors and hiring managers in making decisions about which types of positions they should use in their privacy offices, designing Federal privacy positions, then conducting recruitment and selection activities. You should apply whatever customization of this material is necessary to suit your needs, but the "menu" style of this toolkit provides you with a wide frame of reference to work with to determine your recruitment approach and selection process.

This toolkit can be used to develop a staffing plan, position descriptions, job announcements, and interview questions for a variety of positions, including:

- Senior Agency Officials for Privacy (SAOP SES level work);
- Chief Privacy Officers (CPO):
- privacy counsel;
- privacy analysts; or
- similar positions focused on designing, implementing, and maintaining a Federal information protection and privacy program.

This material applies to occupational series performing privacy work at any grade level within the organization from GS 5-15 or equivalent, and the Senior Executive Service.

This is not a Federal hiring guide. This toolkit does not provide policy guidance on classification, recruitment, hiring and/or assessment. Please consult your agency human resource office for assistance with Federal hiring practices. Additional guides and tools for collecting information on individuals for the purpose of making selection decisions are available at the Office of Personnel Management's Recruitment Policy Studio, https://hru.gov/Studio Recruitment/Studio Recruitment.aspx.

- Hiring Toolkit:
 - o <u>https://hru.gov/Studio_Recruitment/HT_Hiring_Toolkit.aspx</u>
- Hiring Decision Tool

 https://hru.gov/Studio Recruitment/HT Hiring Decision Tool.aspx
- Assessment and Selection Policy
 - o https://www.opm.gov/policy-data-oversight/assessment-and-selection/.

Contents

Position Design	Recruitment Selection	

I. Background	
A. Privacy	4
B. Privacy Programs in the Federal Government	
C. Privacy Laws and Regulations	
II. Position Design	
A. Position Management	7
B. Classifying Privacy Positions	
1. DETERMINING THE PAY SYSTEM	
2. DETERMINING OCCUPATIONAL SERIES OF POSITIONS WITH PRIVACY WORK	8
a) Impact of the Person on the Job	10
b) Occupations Performing and Supporting Privacy Work	
c) OPM Flysheets for Privacy-Related Positions	
GOVERNMENT INFORMATION SERIES, GS-0306	12
MANAGEMENT AND PROGRAM ANALYSIS SERIES, GS-0343	
GENERAL ATTORNEY SERIES, GS-0905	14
INFORMATION TECHNOLOGY MANAGEMENT, GS-2210	
3. DETERMINING OFFICIAL POSITION TITLES	
5. IDENTIFYING POSITIONS ABOVE THE GS-15 GRADE LEVEL: PRIVACY PROGRAM LEADERSHIP	17
6. DESIGNING THE RIGHT POSITION DESCRIPTION.	
III. Recruitment	26
A. Developing Job Opportunity Announcements	
B. Possible Recruitment Sources	
1. HIRING AUTHORITIES AND FLEXIBILITIES	
2. RECRUITMENT RESOURCES	31
IV. Candidate Selection	
A. Qualifying and Ranking Applicants	
1. QUALIFYING APPLICANTS	
2. RANKING QUALIFIED APPLICANTS – QUALITY RANKING FACTORS	
B. Relevant Educational Backgrounds	
1. PRIVACY SPECIALIST, 0306 SERIES AND PRIVACY ANALYST, 343 SERIES	
2. INFOSEC/PRIVACY SPECIALIST, 2210	
3. Attorney 0905 Series	37

5. CERTIFICATIONS 38 C. Support from Privacy Subject Matter Experts 39 D. Assessment Policy and Tools 40 1. POLICY 41 2. TOOLS 41 42 E. General Interview Guidelines for Privacy Positions 42 1. PRE-INTERVIEW PROVIDING INTERVIEWEES WITH SUFFICIENT INFORMATION AND INSIGHT 42 2. INTERVIEW: PROVIDING INTERVIEWEES WITH SUFFICIENT INFORMATION AND INSIGHT 42 a) General Interview Questions for Interns and Entry-Level Positions 43 b) General Interview Questions for Mid- to Senior-Level Candidates 44 c) Leadership of Privacy Program, Job Series 306, 905 and 2210 46 F. Additional Recruiting and Hiring Resources 46 Appendix - Sample Org Structures, PDs, JOAs, Competencies and Interview Questions 47 Appendix A: Sample Organizational Structures for Federal Privacy Programs 48 1. Department or Larger Agency 48 10 2. Independent or Smaller Agency: 48 49 3. Department or Larger Agency (Reporting through CIO) 50 Appendix B: Samples and Templates for Government Information Specialist (Chief Privacy 51 1. 0306: Sample Position Description 51 53 0306 <t< th=""><th>4. CONTINUING EDUCATION COURSES OR PROGRAMS</th><th></th></t<>	4. CONTINUING EDUCATION COURSES OR PROGRAMS	
D. Assessment Policy and Tools 40 1. POLCY 41 2. TOOLS 41 41 E. General Interview Guidelines for Privacy Positions 42 1. PRE-INTERVIEW: PROVIDING INTERVIEW USESTIONS 42 2. INTERVIEW: PROVIDING INTERVIEW QUESTIONS 42 a) General Interview Questions for Mid- to Senior-Level Candidates 44 c) Leadership of Privacy Program, Job Series 306, 905 and 2210 46 F. Additional Recruiting and Hiring Resources 46 Appendix - Sample Org Structures, PDs, JOAs, Competencies and Interview Questions 47 Appendix A: Sample Organizational Structures for Federal Privacy Programs 48 1. Department or Larger Agency 48 2. Independent or Smaller Agency: 49 3. Department or Larger Agency (General Counsel as SAOP) 49 4. Department or Larger Agency (Reporting through CIO) 50 Appendix B: Samples and Templates for Government Information Specialist (Chief Privacy 51 0. 0306: Sample Ab Announcement 55 0. 0306: Sample Competencies and Interview Questions 62 Appendix C: Program Analyst (CPO, Privacy Analyst or Privacy Program Analyst), GS-0343.67 71 1. 0343: Sample Position Description		
1. POLICY 41 2. TOOLS 41 41 E. General Interview Guidelines for Privacy Positions 42 1. PRE-INTERVIEW: PROVIDING INTERVIEWEES WITH SUFFICIENT INFORMATION AND INSIGHT 42 a) General Interview Questions for Interns and Entry-Level Positions 43 b) General Interview Questions for Interns and Entry-Level Positions 44 c) Leadership of Privacy Program, Job Series 306, 905 and 2210 46 F. Additional Recruiting and Hiring Resources 46 Appendix – Sample Org Structures, PDs, JOAs, Competencies and Interview Questions 47 Appendix A: Sample Organizational Structures for Federal Privacy Programs 48 1. Department or Larger Agency: 49 3. Department or Larger Agency (General Counsel as SAOP) 49 4. Department or Larger Agency (Reporting through CIO) 50 Appendix B: Samples and Templates for Government Information Specialist (Chief Privacy Officer or Privacy Specialist), CS-0306 51 1. 0306: Sample Position Description 51 2. 0306: Sample Job Announcement 55 3. 0306: Sample Job Announcement 71 3. 0343: Sample Competencies and Interview Questions 78 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-034367 </td <td></td> <td></td>		
2. Toots 41 E. General Interview Guidelines for Privacy Positions 42 1. PRE. NITER VIEW: PROVIDING INTERVIEWEES WITH SUFFICIENT INFORMATION AND INSIGHT 42 2. INTERVIEWS: POSSIBLE GENERAL INTERVIEW QUESTIONS. 42 a) General Interview Questions for Interns and Entry-Level Positions 43 b) General Interview Questions for Interns and Entry-Level Positions 43 c) Leadership of Privacy Program, Job Series 306, 905 and 2210 46 F. Additional Recruiting and Hiring Resources 46 Appendix – Sample Org Structures, PDs, JOAs, Competencies and Interview Questions 47 Appendix A: Sample Organizational Structures for Federal Privacy Programs 48 1. Department or Larger Agency 48 2. Independent or Smaller Agency: 49 3. Department or Larger Agency (General Counsel as SAOP) 49 4. Department or Larger Agency (General Counsel as SAOP) 49 4. Department or Larger Agency (Reporting through CIO) 50 Appendix B: Samples and Templates for Government Information Specialist (Chief Privacy Officer or Privacy Specialist), GS-0306 51 0. 0306: Sample Position Description 51 0306: Sample Job Announcement 51 0. 0306: Sample Job Announcement 71 3. 0343: Sample Competencies and Int		
1. PRE-INTERVIEW: PROVIDING INTERVIEWERS WITH SUFFICIENT INFORMATION AND INSIGHT		
2. INTERVIEWS: POSSIBLE GENERAL INTERVIEW QUESTIONS 42 a) General Interview Questions for Interns and Entry-Level Positions 43 b) General Interview Questions for Mid- to Senior-Level Candidates 44 c) Leadership of Privacy Program, Job Series 306, 905 and 2210 46 F. Additional Recruiting and Hiring Resources 46 Appendix – Sample Org Structures, PDs, JOAs, Competencies and Interview Questions 47 Appendix A: Sample Organizational Structures for Federal Privacy Programs 48 1. Department or Larger Agency 48 2. Independent or Smaller Agency: 49 3. Department or Larger Agency (General Counsel as SAOP) 49 4. Department or Larger Agency (Reporting through CIO) 50 Appendix B: Samples and Templates for Government Information Specialist (Chief Privacy Officer or Privacy Specialist), GS-0306 51 1. 0306: Sample Position Description 51 2. 0306: Sample Job Announcement 55 3. 0306: Sample Competencies and Interview Questions 62 Appendix C: Program Analyst (CPO, Privacy Analyst or Privacy Program Analyst), GS-034367 78 Appendix C: Program Analyst (CPO, Privacy Counsel or Senior Privacy Counsel), GS-090582 78 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy	E. General Interview Guidelines for Privacy Positions	
a) General Interview Questions for Interns and Entry-Level Positions 43 b) General Interview Questions for Mid- to Senior-Level Candidates 44 c) Leadership of Privacy Program, Job Series 306,905 and 2210 46 F. Additional Recruiting and Hiring Resources 46 Appendix – Sample Org Structures, PDs, JOAs, Competencies and Interview Questions 47 Appendix A: Sample Organizational Structures for Federal Privacy Programs 48 1. Department or Larger Agency 48 2. Independent or Smaller Agency: 49 3. Department or Larger Agency (General Counsel as SAOP) 49 4. Department or Larger Agency (Reporting through CIO) 50 Appendix B: Samples and Templates for Government Information Specialist (Chief Privacy 51 1. 0306: Sample Position Description 51 2. 0306: Sample Job Announcement 62 Appendix C: Program Analyst (CPO, Privacy Analyst or Privacy Program Analyst), GS-034367 71 3. 0343: Sample Job Announcement 71 3. 0343: Sample Position Description 72 3. 0305: Sample Job Announcement 78 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-034367 78 Appendix D: General Attorney (CPO, Privacy Counsel or Senior		
b) General Interview Questions for Mid- to Senior-Level Candidates		
c) Leadership of Privacy Program, Job Series 306,905 and 2210		
Appendix – Sample Org Structures, PDs, JOAs, Competencies and Interview Questions 47 Appendix A: Sample Organizational Structures for Federal Privacy Programs 48 1. Department or Larger Agency. 48 2. Independent or Smaller Agency: 49 3. Department or Larger Agency (General Counsel as SAOP) 49 4. Department or Larger Agency (Reporting through CIO) 50 Appendix B: Samples and Templates for Government Information Specialist (Chief Privacy Officer or Privacy Specialist), GS-0306 51 1. 0306: Sample Position Description 51 2. 0306: Sample Job Announcement 55 3. 0306: Sample Competencies and Interview Questions 62 Appendix C: Program Analyst (CPO, Privacy Analyst or Privacy Program Analyst), GS-034367 67 2. 0343: Sample Position Description 67 3. 0343: Sample Competencies and Interview Questions 78 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-0905 82 2. 0905: Sample Job Announcement 88 3. 0905: Sample Competencies and Interview Questions 94 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-0905 82 2. 0905: Sample Job Announcement 88 3. 0905: Sample Compe		
Appendix A: Sample Organizational Structures for Federal Privacy Programs 48 1. Department or Larger Agency 48 2. Independent or Smaller Agency: 49 3. Department or Larger Agency (General Counsel as SAOP) 49 4. Department or Larger Agency (Reporting through CIO) 50 Appendix B: Samples and Templates for Government Information Specialist (Chief Privacy Officer or Privacy Specialist), GS-0306 51 1. 0306: Sample Position Description 51 2. 0306: Sample Position Description 55 3. 0306: Sample Competencies and Interview Questions 62 Appendix C: Program Analyst (CPO, Privacy Analyst or Privacy Program Analyst), GS-034367 67 2. 0343: Sample Position Description 67 3. 0343: Sample Lob Announcement 71 3. 0343: Sample Competencies and Interview Questions 78 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-090582 1. 0905: Sample Position Description 2. 0905: Sample Job Announcement 88 3. 0905: Sample Competencies and Interview Questions 94 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-090582 1. 0905: Sample Position Description 2. 0905: Sample Job Announcement 88 3. 090	F. Additional Recruiting and Hiring Resources	
1. Department or Larger Agency. 48 2. Independent or Smaller Agency: 49 3. Department or Larger Agency (General Counsel as SAOP) 49 4. Department or Larger Agency (Reporting through CIO) 50 Appendix B: Samples and Templates for Government Information Specialist (Chief Privacy 51 1. 0306: Sample and Templates for Government Information Specialist (Chief Privacy 51 1. 0306: Sample Position Description 51 2. 0306: Sample Competencies and Interview Questions 62 Appendix C: Program Analyst (CPO, Privacy Analyst or Privacy Program Analyst), GS-034367 67 2. 0343: Sample Position Description 67 2. 0343: Sample Job Announcement 71 3. 0343: Sample Position Description 78 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-0905 82 2. 0905: Sample Position Description 82 3. 0905: Sample Job Announcement 88 3. 0905: Sample Competencies and Interview Questions 94 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-0905 82 2. 0905: Sample Job Announcement 88 3. 0905: Sample Competencies and Interview Questions 94 Appendix	Appendix – Sample Org Structures, PDs, JOAs, Competencies and Interview Question	s47
2. Independent or Smaller Agency: 49 3. Department or Larger Agency (General Counsel as SAOP) 49 4. Department or Larger Agency (Reporting through CIO) 50 Appendix B: Samples and Templates for Government Information Specialist (Chief Privacy Officer or Privacy Specialist), GS-0306 51 1. 0306: Sample Position Description 51 2. 0306: Sample Job Announcement 55 3. 0306: Sample Competencies and Interview Questions 62 Appendix C: Program Analyst (CPO, Privacy Analyst or Privacy Program Analyst), GS-034367 67 2. 0343: Sample Position Description 67 3. 0343: Sample Competencies and Interview Questions 78 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-0905 82 1. 0905: Sample Position Description 82 2. 0905: Sample Job Announcement 88 3. 0905: Sample Position Description 82 4. Oppendix E: IT Specialist (CPO, INFOSEC/Privacy Specialist, Privacy Program Manager, or Data Lifecycle Management and Privacy Protection), GS-2210 101 1. 2210: Sample Position Description 101 2. 2210: Sample Position Description 101	Appendix A: Sample Organizational Structures for Federal Privacy Programs	
2. Independent or Smaller Agency: 49 3. Department or Larger Agency (General Counsel as SAOP) 49 4. Department or Larger Agency (Reporting through CIO) 50 Appendix B: Samples and Templates for Government Information Specialist (Chief Privacy Officer or Privacy Specialist), GS-0306 51 1. 0306: Sample Position Description 51 2. 0306: Sample Job Announcement 55 3. 0306: Sample Competencies and Interview Questions 62 Appendix C: Program Analyst (CPO, Privacy Analyst or Privacy Program Analyst), GS-034367 67 2. 0343: Sample Position Description 67 3. 0343: Sample Competencies and Interview Questions 78 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-0905 82 1. 0905: Sample Position Description 82 2. 0905: Sample Job Announcement 88 3. 0905: Sample Position Description 82 4. Oppendix E: IT Specialist (CPO, INFOSEC/Privacy Specialist, Privacy Program Manager, or Data Lifecycle Management and Privacy Protection), GS-2210 101 1. 2210: Sample Position Description 101 2. 2210: Sample Position Description 101	1. Department or Larger Agency	
4. Department or Larger Agency (Reporting through CIO) 50 Appendix B: Samples and Templates for Government Information Specialist (Chief Privacy Officer or Privacy Specialist), GS-0306 51 1. 0306: Sample Position Description 51 2. 0306: Sample Competencies and Interview Questions 62 Appendix C: Program Analyst (CPO, Privacy Analyst or Privacy Program Analyst), GS-034367 67 2. 0343: Sample Position Description 67 3. 0343: Sample Job Announcement 71 3. 0343: Sample Competencies and Interview Questions 78 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-0905 82 1. 0905: Sample Position Description 82 2. 0905: Sample Position Description 82 3. 0905: Sample Competencies and Interview Questions 94 Appendix E: IT Specialist (CPO, INFOSEC/Privacy Specialist, Privacy Program Manager, or Data Lifecycle Management and Privacy Protection), GS-2210 101 1. 2210: Sample Position Description 101 2. 2210: Sample Position Description 101		
Appendix B: Samples and Templates for Government Information Specialist (Chief Privacy Officer or Privacy Specialist), GS-0306 51 1. 0306: Sample Position Description 51 2. 0306: Sample Competencies and Interview Questions 62 Appendix C: Program Analyst (CPO, Privacy Analyst or Privacy Program Analyst), GS-034367 67 2. 0343: Sample Position Description 67 2. 0343: Sample Position Description 67 2. 0343: Sample Competencies and Interview Questions 78 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-0905 82 1. 0905: Sample Position Description 82 2. 0905: Sample Position Description 88 3. 0905: Sample Competencies and Interview Questions 94 Appendix E: IT Specialist (CPO, INFOSEC/Privacy Specialist, Privacy Program Manager, or Data Lifecycle Management and Privacy Protection), GS-2210 101 1. 2210: Sample Position Description 101 2. 2210: Sample Position Description 101	3. Department or Larger Agency (General Counsel as SAOP)	49
Officer or Privacy Specialist), GS-0306 51 1. 0306: Sample Position Description 51 2. 0306: Sample Job Announcement 55 3. 0306: Sample Competencies and Interview Questions 62 Appendix C: Program Analyst (CPO, Privacy Analyst or Privacy Program Analyst), GS-034367 67 2. 0343: Sample Position Description 67 2. 0343: Sample Competencies and Interview Questions 71 3. 0343: Sample Competencies and Interview Questions 78 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-0905 82 1. 0905: Sample Position Description 82 2. 0905: Sample Position Description 82 3. 0905: Sample Competencies and Interview Questions 94 Appendix E: IT Specialist (CPO, INFOSEC/Privacy Specialist, Privacy Program Manager, or 94 Appendix E: IT Specialist (CPO, INFOSEC/Privacy Specialist, Privacy Program Manager, or 101 1. 2210: Sample Position Description 101 2. 2210: Sample Position Description 101 2. 2210: Sample Job Announcement 107	4. Department or Larger Agency (Reporting through CIO)	50
2. 0306: Sample Job Announcement		
2. 0306: Sample Job Announcement	1. 0306: Sample Position Description	
3. 0306: Sample Competencies and Interview Questions 62 Appendix C: Program Analyst (CPO, Privacy Analyst or Privacy Program Analyst), GS-0343.67 67 1. 0343: Sample Position Description 67 2. 0343: Sample Job Announcement 71 3. 0306: Sample Competencies and Interview Questions 78 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-0905 82 1. 0905: Sample Position Description 82 2. 0905: Sample Job Announcement 88 3. 0905: Sample Competencies and Interview Questions 94 Appendix E: IT Specialist (CPO, INFOSEC/Privacy Specialist, Privacy Program Manager, or Data Lifecycle Management and Privacy Protection), GS-2210 101 1. 2210: Sample Position Description 101 2. 2210: Sample Job Announcement 101		
1. 0343: Sample Position Description 67 2. 0343: Sample Job Announcement 71 3. 0343: Sample Competencies and Interview Questions 78 Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-0905 82 1. 0905: Sample Position Description 82 2. 0905: Sample Job Announcement 88 3. 0905: Sample Competencies and Interview Questions 94 Appendix E: IT Specialist (CPO, INFOSEC/Privacy Specialist, Privacy Program Manager, or Data Lifecycle Management and Privacy Protection), GS-2210 101 1. 2210: Sample Position Description 101 2. 210: Sample Job Announcement 107	-	
2. 0343: Sample Job Announcement713. 0343: Sample Competencies and Interview Questions78Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-0905821. 0905: Sample Position Description822. 0905: Sample Job Announcement883. 0905: Sample Competencies and Interview Questions94Appendix E: IT Specialist (CPO, INFOSEC/Privacy Specialist, Privacy Program Manager, or1011. 2210: Sample Position Description1012. 2210: Sample Job Announcement107	Appendix C: Program Analyst (CPO, Privacy Analyst or Privacy Program Analyst), G	S-034367
2. 0343: Sample Job Announcement713. 0343: Sample Competencies and Interview Questions78Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-0905821. 0905: Sample Position Description822. 0905: Sample Job Announcement883. 0905: Sample Competencies and Interview Questions94Appendix E: IT Specialist (CPO, INFOSEC/Privacy Specialist, Privacy Program Manager, or1011. 2210: Sample Position Description1012. 2210: Sample Job Announcement107	1. 0343: Sample Position Description	
Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-090582 1. 0905: Sample Position Description		
1. 0905: Sample Position Description 82 2. 0905: Sample Job Announcement 88 3. 0905: Sample Competencies and Interview Questions 94 Appendix E: IT Specialist (CPO, INFOSEC/Privacy Specialist, Privacy Program Manager, or Data Lifecycle Management and Privacy Protection), GS-2210 101 1. 2210: Sample Position Description 101 2. 2210: Sample Job Announcement 107	3. 0343: Sample Competencies and Interview Questions	
2. 0905: Sample Job Announcement	Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS	-090582
2. 0905: Sample Job Announcement	1. 0905: Sample Position Description	
Appendix E: IT Specialist (CPO, INFOSEC/Privacy Specialist, Privacy Program Manager, or Data Lifecycle Management and Privacy Protection), GS-2210 1. 2210: Sample Position Description 2. 2210: Sample Job Announcement		
Data Lifecycle Management and Privacy Protection), GS-22101011. 2210: Sample Position Description1012. 2210: Sample Job Announcement107	3. 0905: Sample Competencies and Interview Questions	
1. 2210: Sample Position Description		0
2. 2210: Sample Job Announcement 107		
-		

I. Background

A. Privacy

Privacy is difficult to define because it is truly multifaceted, involving law, policy and technology. Privacy in the United States includes the constitutional right of individuals "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. Fourth Am. Privacy includes the "right of the individual . . . to be free from unwanted governmental intrusions." <u>Eisenstadt v. Baird</u>, 405 U.S. 438, 453 (1972). Privacy includes guarding information about individuals from unauthorized interference or disclosure, and mitigating risks to that information throughout the information life cycle, whether information is in paper or electronic form. Privacy also includes the evolving relationship between technology and the legal right to, or public expectation of, some level of control over the collection and use of information about oneself, for example, being notified about the type of information being collected and how that information may be used and disclosed, and making decisions about collection and sharing data about one's self.

B. Privacy Programs in the Federal Government

Privacy professionals in the Government have a vast array of responsibilities under dozens of federal laws, regulations, standards, and policy mandates from the Office of Management and Budget (OMB).¹ The mandates that privacy officials implement or on which they advise agency leadership arise under the Constitution's Fourth Amendment, the Privacy Act of 1974, the E-Government Act of 2002, the Federal Information Security Modernization Act of 2014, and OMB Circular A-130, OMB Circular A-108, OMB M-17-12 and other guidance, in addition to international privacy-related laws that may impact an agency's mission, and many agency- and sector-specific laws and obligations, including the Bank Secrecy Act, Electronic Communications Privacy Act, and laws in the health, education, and financial sectors. Mandates also include privacy-related information technology requirements and standards, for example, identity management, cloud computing, encryption, mobile app security, data analytics, and access controls. The leaders of privacy programs bear additional responsibility. As explained below, by law, each agency must designate a Senior Agency Official for Privacy who is accountable for the program, must have a central policy-making role, and must ensure that the agency considers the privacy impact of all agency actions and policies that involve personally identifiable information.

Privacy is a robust and rapidly growing multidisciplinary field that attracts lawyers, IT professionals and cybersecurity experts, professors and academics, and other professionals with diverse backgrounds and advanced education, not only for Government privacy positions but also for non-Governmental, not-for-profit, and private sector positions.²

¹ The Privacy Act of 1974 directs OMB to develop and prescribe guidelines and regulations for agencies in implementing the Act and to provide assistance and oversight of implementation. Privacy Act, 5 U.S.C. 552a(v). ² Many organizations and corporations -- both large and small -- have Chief Privacy Officers, and law firms and consulting practices have practice groups servicing even more. One professional organization, the International Association of Privacy Professionals (IAPP), has more than 25,000 active members in 83 countries, including many Government employees. See, e.g., https://iapp.org/about/iapp-facts.

<u>C. Privacy Laws and Regulations</u>

Federal Privacy Programs follow a complex variety of Federal Government laws, regulations, and policies. OMB Circular A-130, substantially revised in 2016, outlines many of the responsibilities of Federal privacy offices. Privacy offices must recruit individuals with a variety of skillsets to successfully achieve the mandates in this Circular. In addition, Federal agencies follow a multitude of other privacy laws, depending on their industry sector requirements.

Significant Privacy Related Laws and Regulations
Bank Secrecy Act
Cable Act
Children's Online Privacy Protection Act
Confidential Information Protection and Statistical Efficiency Act
Cybersecurity Information Sharing Act
Department of Justice Regulations, e.g., Criminal Justice Information Systems
E-Government Act
Electronic Communications Privacy Act
Fair Credit Reporting Act
Family Educational Rights and Privacy Act
Federal Information Security Modernization Act
Federal Records Act
Foreign Intelligence Surveillance Act
Freedom of Information Act
Gramm-Leach Bliley Act
Health Insurance Portability and Accountability Act
Internal Revenue Code
National Institute of Standards and Technology
Office of Management and Budget (OMB) Circular A-130 (revised July 2016)
OMB Circular A-108 (revised Dec. 2016)
OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy
OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (released Jan. 2017)
OMB Additional Memoranda and Guidance
Privacy Act
Paperwork Reduction Act
Right to Financial Privacy Act

Statistical Information
Social Security Act
Telecommunication Act
USA Freedom Act
Video Privacy Protection Act
Wiretap Act

II. Position Design

In support of the Open Government Act 2007 and a renewed commitment to transparency in the Federal Government, the U.S. Office of Personnel Management (OPM) established the Government Information Series, 0306 (March 2012) on the classification of positions responsible for administering the Freedom of Information Act (FOIA) and Privacy Act of 1974 (PA). OPM released the Position Classification Flysheet for the Government Information Series 0306 (March 2012) in support of the White House commitment to transparency and accountability.

Since the new series was established, however, the role of Federal privacy offices has become more complex. While this classification series has worked well for hiring candidates into positions focused on FOIA compliance, members of the Federal Privacy Council have faced challenges in its use for positions in Federal privacy programs, due to the focus of the series on FOIA and, for privacy, only the Privacy Act, and/or due to agency implementation of the series. This toolkit seeks to help Federal agency human resources staff and hiring managers for privacy offices develop appropriate staffing plans for privacy offices that are based on an understanding of the multidisciplinary nature of privacy work.

A. Position Management

The first step in recruiting and hiring privacy professionals is developing a good position management plan. The law (5 U.S.C. Chapter 51) which governs the classification system clearly places upon agencies the authority and responsibility to establish, classify, and manage their own positions.

Position Management is a carefully designed position structure which blends the skills and assignments of employees with the goal of successfully carrying out the organization's mission or program.

Since supervisors and managers play major roles in the management and classification of subordinate positions, they are responsible for assuring a sound position structure in the organizations they lead. The Federal classification system allows considerable freedom and flexibility for Federal managers to establish an organizational structure that is not only efficient but also cost conscious.

Both HR specialists and hiring managers play a role in in the management and classification of subordinate positions. This includes ensuring position descriptions are up to date and include the required duties, responsibilities, and competencies to accomplish the agency's missions and goals.

Note: Agencies may determine the organizational structure of their privacy programs, including the correct distribution of a variety of positions needed to successfully achieve and perform the privacy goals of the agency and government wide. Hiring managers should work with the human resources managers to evaluate the correct classification of the positions within their office, the correct pay plan, and the correct distribution of job series that may be needed to carry out a successful privacy program for their Federal agency, and develop a position management plan that plans for the correct distribution of work across the series and across the office.

B. Classifying Privacy Positions

When classifying a position, the following must be determined:

- The proper pay system;
- The proper occupational series;
- The official position title; and
- The proper grade or level of work.

<u>1. Determining the Pay System</u>

Positions with privacy responsibilities usually are General Schedule (GS) positions. However, some positions may be Senior Executive Service (SES) positions or Senior Level (SL) positions. Guidance for identifying such positions above the GS-15 grade level can be found later in this section. This guidance is not intended for Federal Wage System (FWS) positions. The classification of a position is used to determine certain pay entitlements of an employee in that position. Agencies should remain aware that changes in the pay system, occupational series, title, or grade level of a position could affect how an employee in that position will be paid. For example, coverage under special rates established under 5 U.S.C. 5305 and 5 C.F.R. part 530, subpart C, is dependent on the position's pay system, occupational series, grade level, and, at times, official title.

2. Determining Occupational Series of Positions with Privacy Work

The privacy workforce is multifaceted, encompasses a variety of contexts and roles, and is comprised of a cadre of different backgrounds and experience in order to perform the privacy work required by agencies. There are multiple factors to consider when designing a technically sound organizational structure. Agencies may design their organizations based on their program and mission needs. The proper classification of privacy work performed in agencies must be determined by proper application of the Office of Personnel Management Position Classification Standards. When privacy work is included in other established occupations and covered by more than one occupational series, a classification determination can be made by reviewing the duties and responsibilities assigned to the position. In most instances, the primary work of the position, the highest level of work performed, and the paramount occupational knowledge for the work dictate the appropriate series.

Users of the position classification standards normally have little trouble making the series decision by comparing the characteristics of the position in question to series definitions and occupational information in the standards. However, if the work of a position falls into more than one series, the correct series is sometimes difficult to determine. If it is unclear whether a particular series predominates, consider the following to determine the appropriate series:

• *Paramount occupational knowledge required.* Some positions may include several different kinds of work; however, most positions have a paramount occupational

knowledge requirement in addition to the privacy knowledge, skills, and abilities/competencies. The paramount occupational knowledge is the most important subject matter knowledge or subject-related experience required to do the work.

- *Reason for existence.* The primary purpose for the existence of the position, or management's intent in establishing the position, is a positive indicator in determining the appropriate series.
- **Organizational mission and/or function.** Since privacy is critical work within an organization, privacy may generally be aligned with the mission and function of the organization to which it is assigned. The organization's function often is mirrored in the organizational title and may influence the choice of appropriate series.
- *Recruitment source.* Supervisors and managers can help by identifying the occupational series that provides the best qualified applicants to do the work. This aspect correlates with the paramount knowledge required by the position.

Privacy work can be characterized as multidisciplinary. A multidisciplinary position is a position involving duties and responsibilities closely related to more than one discipline. As a result, the position could be classifiable to two or more occupational series. The nature of the work is such that persons with training and experience in either of two or more occupations may be considered well qualified to do the work.

Note: Due to the evolution of work in privacy, the term multidisciplinary is used to more appropriately define the unique and occupationally cross-cutting combinations of work in this discipline. <u>While this term is not addressed in the current Introduction to the Position</u> <u>Classification Standards or the Classifier's Handbook, future updates will address the usage of this terminology</u>.

Multidisciplinary positions generally fall into one of the following two categories:

- Positions which involve a specific *combination* of knowledges that is characteristic of two or more non-professional series. Such positions involve the performance of some duties which are characteristic of one series and other duties which are characteristic of another series.
- Positions which involve knowledge which is characteristic of *either* two or more nonprofessional series. These positions include work which is substantially identical to work performed in either of the non-professional occupations.

The position description should show clearly that the position is multidisciplinary and indicate the various series in which the position may be classified. This may be determined by completing a job analysis and by employing sound position management. In such cases it may be determined that the work in the office may be performed by individuals from different backgrounds in various disciplines, which provide the individual with transferrable skills or competencies to perform the core functions of the position. The final classification of the position is based on the organization's needs and mission. Section 2, Determining Occupational

<u>Series of Positions with Privacy Work</u>, provides additional guidance on determining the occupational series.

Positions are not to be considered multidisciplinary when members of a work team with varied but complimentary competencies and experiences collaborate on a multifaceted problem or project and contribute to the achievement of organizational specific objectives. Also excluded are positions which require special licensing, as in the practice of medicine, and positions which are solely and clearly classifiable to a single series but can be filled by persons from a variety of education and experience backgrounds. Work requiring professional backgrounds including education and experience are considered interdisciplinary. Professional occupations may not be combined with non-professional occupations or viewed as interdisciplinary positions. For further guidance on interdisciplinary positions reference the discussion on Interdisciplinary.

a) Impact of the Person on the Job

The duties and responsibilities of a position may change over time. For the most part, these changes result from reorganizations, new or revised organizational responsibilities or missions, and changes in technology. Sometimes, however, the unique capabilities, experience, or knowledge a particular employee brings to the job can also have an effect on the work performed and therefore on the classification of the position.

While it is the position which is classified, the relationship of the employee to the position can be recognized when the performance of the incumbent broadens the nature or scope and effect of the work being performed. For example, exceptional ability of the employee may lead to the attraction of especially difficult work assignments, unusual freedom from supervision, special authority to speak for and commit the agency, continuing contribution to organizational efficiency and economy, recognition as an "expert" sought out by peers, or similar considerations. Such changes affect the difficulty of work or the responsibility and authority given the employee and can be recognized in the position classification decision.

Job changes resulting from the individual impact of an employee should be recorded to distinguish the position from descriptions of other positions.

When significant changes in work occur for any of the kinds of reasons mentioned above, the classification of the position (title, series, and grade) should be reviewed and revised as needed. When a position which has been affected by the impact of an individual is vacated, it should normally revert to its original classification.

b) Occupations Performing and Supporting Privacy Work

The following occupational series are most often used by agencies for employees who directly support their agencies' privacy program.

Job Series	Official OPM Title	Organizational/Functional/Parenthetical Title	Grades
0306	Government Information	SAOP; Chief Privacy Officer; Privacy	9-15
	Specialist	Specialist	
0343	Management Analyst;	SAOP; Chief Privacy Officer; Privacy	9 - 15
	Program Analyst;	Analyst; Privacy Program Analyst	
	Management and Program		
	Analyst		
0905	General Attorney	SAOP; Chief Privacy Officer; Privacy	11-15
		Counsel; Sr. Privacy Counsel	
2210	Information Technology (IT)	SAOP; Chief Privacy Officer;	5 -15
	Program Manager; IT Project	INFOSEC/Privacy Specialist; Privacy	
	Manager; IT Specialist	Program Manager; Data Life Cycle	
		Management and Privacy Protection	

Below is information from the official OPM Fly-Sheets for the above occupational series.

c) OPM Flysheets for Privacy-Related Positions

GOVERNMENT INFORMATION SERIES, GS-0306

Government information work involves implementing policies and procedures to manage Government information and providing information-related assistance and services to the general public. The work requires interpreting and applying laws, regulations, policies, and guidance to provide access to Federal agency records and information, while ensuring protected information is appropriately disclosed. Government Information Specialists make determinations about disclosures, issuance of denials, redactions, access to Federal agency records and use and dissemination of personally identifiable information. Many Government information specialists focus on Freedom of Information Act (FOIA), Privacy Act, or a combination of both.

Typical work related to the Privacy Act includes:

- developing, implementing, and maintaining privacy policies and procedures;
- processing Privacy Act data requests;
- providing guidance and advice on Federal privacy policy and processes;
- evaluating confidential personal records that, if released, would constitute an unwarranted invasion of personal privacy;
- evaluating the impact of the Privacy Act and regulations on the organization's activities;
- coordinating with internal organizations, such as the agency's information technology security office;
- representing the agency on issues related to the Privacy Act and other information privacy requirements;
- assessing privacy risks associated with programs, operations, and technology;
- ensuring compliance with agency privacy program requirements;
- planning and conducting educational training sessions on Privacy Act requirements; or reviewing and evaluating the privacy program.

Note: Above is the Fly-Sheet for the 0306 position. This list of duties and responsibilities is not all inclusive. Positions in a privacy program involve responsibilities not only under the Privacy Act, but under dozens of other laws and requirements. OPM will continue to study privacy work in the Federal Government to consider any needed updates to current policy and other guidance needed by agencies to properly fill privacy positions government-wide. Until additional policy guidance is available for agency use and implementation, this toolkit may be used as a resource to agencies designing positions and filling privacy positions.

Since the creation of the 0306 series in 2012 the work roles of the privacy program have evolved due to the expansion of the laws that govern privacy work in the Federal Government, concerns about alleged over-collection or misuse of personal information for law enforcement and anti-terrorism purposes, and the need to protect the privacy of information being shared due to cyber attacks and other privacy-related risks. Therefore, privacy program managers are encouraged to consider using multiple series within their offices to assure that issues related to law, policy, and technology are adequately covered. The descriptions for these related series follow.

MANAGEMENT AND PROGRAM ANALYSIS SERIES, GS-0343

This series includes positions that primarily serve as analysts and advisors to management on the evaluation of the effectiveness of government programs and operations or the productivity and efficiency of the management of Federal agencies or both. Positions in this series require knowledge of: the substantive nature of agency programs and activities; agency missions, policies, and objectives; management principles and processes; and the analytical and evaluative methods and techniques for assessing program development or execution and improving organizational effectiveness and efficiency. Some positions also require an understanding of basic budgetary and financial management principles and techniques as they relate to long range planning of programs and objectives. The work requires skill in: application of factfinding and investigative techniques; oral and written communications; and development of presentations and reports. It also involves:

- analyzing and evaluating (on a quantitative or qualitative basis) the effectiveness of line program operations in meeting established goals and objectives;
- developing life cycle cost analyses of projects or performing cost benefit or economic evaluations of current or projected programs;
- advising on the distribution of work among positions and organizations and the appropriate staffing levels and skills mix;
- advising on the potential benefits/uses of automation to improve the efficiency of administrative support or program operations;
- evaluating and advising on the organization, methods, and procedures for providing administrative support systems such as records, communications, directives, forms, files, and documentation;
- researching and investigating new or improved business and management practices for application to agency programs or operations;
- analyzing management information requirements to develop program or administrative reporting systems including the systems specifications, data gathering and analytical techniques, and systems evaluation methodology;
- analyzing new or proposed legislation or regulations to determine impact on program operations and management;
- developing new or modified administrative program policies, regulations, goals, or objectives;
- identifying data required for use in the management and direction of programs;
- developing data required for use in the management and direction of programs;
- developing management and/or program evaluation plans, procedures, and methodology;
- and conducting studies of employee/organizational efficiency and productivity and recommending changes or improvements in organization, staffing, work methods, and procedures.

Note: As noted for the 0306 job series, above is the Fly-Sheet for the GS-0343. This list of duties and responsibilities is not all inclusive.

GENERAL ATTORNEY SERIES, GS-0905

This series includes professional legal positions involved in preparing cases for trial and/or the trial of cases before a court or an administrative body or persons having quasi-judicial power; rendering legal advice and services with respect to questions, regulations, practices, or other matters falling within the purview of a Federal Government agency (this may include conducting investigations to obtain evidentiary data); preparing interpretive and administrative orders, rules, or regulations to give effect to the provisions of governing statutes or other requirements of law; drafting, negotiating, or examining contracts or other legal documents required by the agency's activities; drafting, preparing formal comments, or otherwise making substantive recommendations with respect to proposed legislation; editing and preparing for publication statutes enacted by Congress and opinions or decisions of a court, commission, or board; and drafting and reviewing decisions for consideration and adoption by agency officials. Included also are positions, not covered by the Administrative Procedure Act, involved in hearing cases arising under contracts or under the regulations that have the effect of law, and rendering decisions or making recommendations for disposition of such cases. The work of this series requires admission to the bar.

INFORMATION TECHNOLOGY MANAGEMENT, GS-2210

This series covers two-grade interval administrative positions that manage, supervise, lead, administer, develop, deliver, and support information technology (IT) systems and services. This series covers only those positions for which the paramount requirement is knowledge of IT principles, concepts, and methods, e.g., data storage, software applications, networking.

Title 5, United States Code, requires the U.S. Office of Personnel Management (OPM) to establish the authorized official position titles which include a basic title (e.g., Information Technology Specialist) that may be appended with one or more prefixes and/or suffixes. Agencies must use official position titles for human resources management, budget, and fiscal purposes. Instructions for assigning official position titles are provided in this section.

The basic titles for this occupation are:

IT Program Manager - Work that involves managing one or more major multi-year IT initiatives of such magnitude they must be carried out through multiple related IT projects. The IT Program Manager leads, coordinates, communicates, integrates and is accountable for the overall success of the program, ensuring alignment with critical agency priorities. They are responsible for ensuring the work efforts achieve the outcome specified within the agency's business strategy, including appropriate strategic, life cycle management, and capital IT investment plans. Work includes project selection, prioritization, evaluation and monitoring, cost schedule management, risk management, quality management, and resource allocations.

IT Project Manager - Work that involves directly managing information technology projects to provide a unique service or product. (**Note**: See Interpretive Guidance for Project Managers for evaluation criteria and information regarding this work.)

Information Technology Specialist or *IT Specialist* – Work that involves developing, delivering, and supporting IT systems and services is *Information Technology Specialist* or *IT Specialist*. Use the parenthetical specialty titles defined below with the basic title to further identify the duties and responsibilities performed and the special knowledge and skills needed.

Use the parenthetical specialty titles defined below with the basic title to further identify the duties and responsibilities performed and the special knowledge and skills needed. OPM has prescribed eleven parenthetical titles for the Information Technology Management series, 2210, covered by this Job Family Standard (JFS):

Policy and Planning	Systems Administration
Network Services	Applications Software
Enterprise Architecture	Customer Support
Data Management	Operating Systems
Security	
Internet	
Systems Analysis	

Agencies must manage information and information systems in ways that address and mitigate security and privacy risks. While security and privacy are not the same, they overlap in key ways. An agency cannot have privacy without security, i.e., to protect privacy rights, information must be controlled and secured. Any privacy program must have professionals who understand and ensure compliance with information technology requirements. Privacy program staff must understand privacy impacts of technology, and risks to data as it moves into, through and out of systems, from initial collection of data through its storage, use, processing, transfer, dissemination, and ultimate disposition. Privacy staff also must be able to translate cybersecurity and privacy regulations and policies into technical solutions that support privacy and an agency's mission.

3. Determining Official Position Titles

The law, 5 U.S.C. 5105 (a)(2), requires OPM to establish the official titles of positions in published classification standards. Accordingly, position classification standards generally prescribe the titles to be used for positions in the covered series. Only the prescribed title may be used on official documents relating to a position (e.g., positon descriptions and personnel actions).

The requirement to use official titles, 5 U.S.C. 5105(c), however, does not preclude agencies from using any unofficial title they choose for positions. Agencies may use organizational or other titles for internal administration, public convenience, or similar purposes.

In those instances where OPM has not prescribed an official title for a series, an agency may designate an official title. According to the **Introduction to the Position Classification Standards**, constructed titles should be "short," "meaningful," and "generally descriptive of the work performed." All titling should be used consistently throughout the agency.

Titling Guidance for 306 Government Information Occupational Series Positions

The 306 Series includes the basic or official title, Government Information Specialist. As mentioned above, the requirement to use official titles under 5 U.S.C. 5105(c), does not preclude agencies from using any unofficial title they choose for positions. Agencies may use organizational or other titles for internal administration, public convenience, or similar purposes. The parenthetical titles may supplement an official or basic title and should only be used when the position requires work characterized by the parenthetical title. In application a 306 position may include the following basic title and parenthetical title: Government Information Specialist (Privacy).

Titling Guidance for other Occupational Series including Privacy Duties

Agencies with positions including privacy work as outlined in this guidance may supplement the basic position titles by adding parenthetical titles, where necessary, to identify privacy duties and

responsibilities which reflect specific privacy knowledge and skills required in the work. Parenthetical titles may be necessary for recruitment purposes and meeting other organizational needs. For example agencies may supplement the basic position titles by adding parenthetical titles, e.g., for the Management and Program Analysis 343 Series, Management and Program Analyst (Privacy Analyst).

Official Specialty or Parenthetical Titles

In addition to this titling guidance agencies may also use specialty titles. Specialty titles are typically displayed in parentheses and referred to as parenthetical titles as well. Parenthetical titles, as defined above, may be used with the basic/official title of the position to further identify the duties and responsibilities performed and the special knowledge and skills needed.

Agencies should use the basic/official title without a parenthetical specialty title for positions with no established specialty or emphasis area or for positions involving work in more than two of the established specialties.

Organizational Titles

Organizational and functional titles do not replace, but complement, official position titles. Agencies may establish organizational and functional titles for internal administration, public convenience, or similar purposes. Examples of organizational titles are Chief Privacy Officer and Cybersecurity Division Chief. Examples of functional titles are Privacy Analyst, Chief Privacy Officer and Director of Privacy and Senior Agency Official for Privacy.

4. Applying Grading Criteria to Privacy Positions

According to the **Introduction to the Position Classification Standards**, selecting the appropriate grade level criteria is critical for determining the proper classification of a position. If the work assigned to a position is adequately covered by the grading criteria in a particular standard for a specific occupational series or job family, then evaluate the work by that occupational series or job family standard (JFS). This includes positions with privacy responsibilities.

If the type of work does not have a directly applicable occupational series, job family, or functional standard, then select a standard as similar as possible to the kind of work described. Evaluate and grade the work in question by comparing it to grading criteria in the comparable standard, as it relates to:

- The kind of work processes, functions, or subject matter of the work performed;
- The qualifications required to do the work;
- The level of difficulty and responsibility necessary; and
- The combination of classification factors having the greatest influence on the grade level.

When making these determinations, we recommend referring to one of the following standards for making meaningful comparisons:

- The <u>Position Classification Flysheet for Government Information Series, 0306</u>, to evaluate positions with privacy roles in establishing, safeguarding, disseminating or managing Government information;
- The <u>Position Classification Flysheet for Records and Information Management</u> <u>Series, 0308</u>, to evaluate positions with privacy roles;
- The <u>Position Classification Flysheet for Management and Program Analysis Series</u>, <u>0343</u>, to evaluate positions with evaluation responsibilities of the effectiveness of government programs and operations or the productivity and efficiency of the management of Federal agencies or both;
- The <u>Position Classification Standard for General Attorney Series</u>, <u>GS-0905</u>, to evaluate positions with professional legal roles;
- The JFS for Administrative Work in the Information Technology Group, GS-2200, to evaluate positions in the IT occupation with privacy responsibilities; and
- The <u>Administrative Analysis Grade Evaluation Guide</u> to evaluate positions with privacy responsibilities where a more closely related standard has not been issued.

Note: If a position with privacy work exercises supervision of Federal Government employees at a level that meets the criteria indicated in <u>General Schedule Supervisory Guide</u>, be sure to evaluate the position's supervisory duties. Do not classify such position to a lower grade on the basis of personal work accomplishment rather than the proper grade for supervising staff of the type and level actually involved.

Example: Government Information Specialist (Privacy Specialist), 0306

FLD 1-7: Privacy Specialist, 0306 (Illustration #1)

Knowledge of and skill in applying:

- agency programs, regulations and policies; the Privacy Act, E-Government Act, and other privacy-related Federal statutes, regulations, policies, and procedures;
- technological advances and privacy safeguards used in the agency; and
- current program and operating objectives and trends.

sufficient to:

- advise agency personnel on privacy-related policies, procedures and controls, including authority to collect, data minimization, notice, consent, access and correction requirements, redress, privacy controls, authority to disclose, data security and incident response to strengthen policies, procedures and controls, and to provide advice and guidance;
- to determine privacy and disclosure decisions; and/or
- analyze and summarize privacy-related issues.

FLD 1-8: Privacy Specialist, 0306 (Illustration #2)

Mastery of and skill in applying:

- tools and methodologies to review, analyze, and evaluate privacy-related issues;
- substantial knowledge of privacy-related policy formulation and implementation, and policies and procedures;
- administrative laws, policies, and Federal laws governing privacy-related matters, including the flow of information and of laws, regulations, policies, precedents, and guidance.

sufficient to:

- initiate and create comprehensive privacy program policies and processes;
- manage agency personally identifiable information, and provide assistance and services to Departmental employees and the general public; and/or
- appropriately collect, provide notice to individuals, protect, and appropriately disclose information; and to make determinations about disclosures and other privacy-related matters.

Using the <u>Administrative Analysis Grade Evaluation Guide</u> to evaluate the duties listed above could result in classifying the position across all nine factors in the Factor Evaluation System as a Privacy Specialist, GS-0306-11:

Factor	Level	Points
1. Knowledge Required	1–7	1,250
2. Supervisory Controls	2–4	450

Federal Privacy Council / OPM

3. Guidelines	3–3	275
4. Complexity	4-4	225
5. Scope & Effect	5–3	150
6 & 7. Contacts & Purpose	3–B/C	180
8. Physical Demands	8-1	5
9. Work Environment	9–1	5
Total Points2,540		2,540
Conversion GS-11		GS-11

Using the <u>Administrative Analysis Grade Evaluation Guide</u> to evaluate the duties listed above could result in classifying the position across all nine factors in the Factor Evaluation System as a Privacy Specialist, GS-0306-12:

Factor	Level	Points
1. Knowledge Required	1–7	1,250
2. Supervisory Controls	2–4	450
3. Guidelines	3–4	450
4. Complexity	4-4/5	225
5. Scope & Effect	5-4/5	225
6 & 7. Contacts & Purpose	3-С	180
8. Physical Demands	8-1	5
9. Work Environment	9–1	5
Total Points2,790		
Conversion GS-12		GS-12

Using the <u>Administrative Analysis Grade Evaluation Guide</u> to evaluate the duties could result in classifying the position across all nine factors in the Factor Evaluation System as a Privacy Specialist, GS-0306-13:

Factor	Level	Points
1. Knowledge Required	1-8	1,550
2. Supervisory Controls	2–4	450
3. Guidelines	3–4	450
4. Complexity	4–5	325
5. Scope & Effect	5–5	325
6 & 7. Contacts & Purpose	3-С	230
8. Physical Demands	8-1	5
9. Work Environment	9–1	5
Total Points3,340		3,340
Conversion GS-13		GS-13

Note: The above tables show examples only. They do not preclude the use of other factor levels that may be appropriate depending on the assignment of duties and responsibilities to a particular position.

5. Identifying Positions above the GS-15 Grade Level: Privacy Program Leadership

In accordance with <u>OMB Memorandum M-16-24 (Role and Designation of Senior Agency</u> <u>Officials for Privacy</u>) and <u>OMB Circular A-130 (Managing Information as a Strategic Resource)</u>, the privacy role ultimately accountable for leadership of the privacy program is the Senior Agency Official for Privacy (SAOP). Under OMB requirements, each agency head must designate a senior official at the Deputy Assistant Secretary or equivalent level to serve as the SAOP. The SAOP develops, implements, documents, maintains, and oversees the agency-wide privacy program that includes people, processes, and technologies. The SAOP is responsible for ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risks consistent with the agency's mission. The SAOP must have a central policy-making role and ensure that the agency considers the privacy impact of all agency actions and policies that involve personally identifiable information (PII). The SAOP's review of privacy risks begins at the earliest planning and development stages of agency actions and policies that involve PII, and continues throughout the lifecycle of the information.

The SAOP must serve in a central leadership position at the agency, must have visibility into relevant agency operations, and must be positioned highly enough within the agency to regularly engage with other agency leadership, including the head of the agency. Moreover, the SAOP must have the necessary skills, knowledge, and expertise to lead and direct the agency's privacy program and carry out the privacy-related functions described in law and OMB policies. At the discretion of the SAOP and consistent with applicable law, other qualified agency personnel (e.g., a Chief Privacy Officer) may perform particular privacy functions that are assigned to the SAOP. Agencies may establish privacy programs and privacy officials at sub-agencies, components, or programs where there is a need for privacy leadership in support of the SAOP. In all cases, however, the SAOP shall retain responsibility and accountability for the agency's privacy programs.

Agencies are responsible for managing their executive resources and deciding how to organize functions and structure positions, including positions with privacy work, in a manner that best meets the organization's mission requirements. This includes deciding whether positions meet the Senior Executive Service (SES) criteria or the Senior Level (SL) or Scientific/Professional (ST) criteria and establishing individual SES, SL, and ST positions within the agency's executive resource allocation as authorized by OPM. Appendix A contains examples of different organizational structures for Federal Government privacy programs.

The law and OPM regulations clearly state that SES, SL, and ST positions must be classifiable **above the GS-15 grade level**. Positions at the GS-15 grade level as described in statute clearly cover a broad range of work: *Grade GS-15 includes those classes of positions the duties of which are to perform, under general administrative direction, with very wide latitude for the exercise of independent judgment, work of outstanding difficulty and responsibility along special technical, supervisory, or administrative lines which has demonstrated leadership and exceptional attainments (5 U.S.C. 5104(15)).* Do not assume a position is above the GS-15 grade level simply

because it has a somewhat larger scope or requires more knowledge and skill than another position with privacy work that is already classified at GS-15.

Distinctions among the SES, SL, and ST positions are not always clear. The following information provides general guidance to help agencies identify SES, SL, and ST positions; maintain an agency's flexibility to manage its executive resources; and contribute to intra- and inter-agency consistency in establishing SES, SL, and ST positions.

General Information - Unless an agency is excluded from the SES by statute or by the President of the United States, any position that is classifiable above the GS-15 grade level **and** which meets the functional executive criteria set forth in 5 U.S.C. 3132(a)(2) may be placed in the SES. Positions that are classifiable above the GS-15 grade level that do **not** meet the executive criteria and involve the performance of high-level research and development in the physical, biological, medical, or engineering sciences are more appropriately placed in the ST system. The SL system includes any other positions that are classifiable above the GS-15 grade level and do **not** meet the executive criteria and do **not** involve the fundamental research and development responsibilities characteristic of ST positions.

SES Criteria - 5 U.S.C. 3132(a)(2) sets forth the criteria that characterize SES positions. SES positions must be classifiable **above the GS-15 grade level**, or equivalent, based on the duties, responsibilities, and qualifications required by the position. In addition, the incumbent **must** engage in one of the following activities:

- Directing the work of an organizational unit;
- Being accountable for the success of one or more specific programs or projects;
- Monitoring progress toward organizational goals and periodically evaluate and make appropriate adjustments to such goals;
- Supervising the work of employees (other than personal assistants); or
- Otherwise exercising important policy-making, policy-determining, or other executive functions.

Directing the work of an organizational unit to manage a program includes responsibility for:

- Assessing policy, program, and project feasibility;
- Determining program goals and developing implementation tools;
- Designing an organizational structure to promote effective work accomplishment; and
- Setting effectiveness, efficiency, productivity, and management/internal control standards.

Being accountable for the success of a program that encompasses responsibility for the full range of factors that affect privacy program management along with a privacy role and accomplishments. This includes:

- Obtaining the resources necessary to achieve the desired program objective;
- Assuming responsibility for the effective use of government resources; and
- Dealing with key officials both within and outside the organization to gain understanding and support for all aspects of the program and program functions.

Monitoring progress toward organizational goals and making appropriate adjustments is an extension of an individual's responsibility for directing the work of an organizational unit. It includes:

- Monitoring work status through formal and informal means to evaluate progress toward objectives;
- Assessing overall effectiveness, efficiency, and productivity of the organization;
- Identifying, diagnosing, and consulting on problem areas related to implementation and goal achievement; and
- Making decisions regarding alternative courses of action.

Supervising the work of employees should be credited only if the position meets the minimum requirements for coverage under OPM's <u>General Schedule Supervisory Guide</u>. Specifically, the position's supervisory responsibilities must:

- Require accomplishment of work through the combined technical and administrative direction of others;
- Constitute a major duty occupying at least 25 percent of the incumbent's time; and
- Meet at least the lowest level of Factor 3 in the guide based on supervision of noncontractor personnel. (Work performed by contractors is considered in applying the grading criteria within each factor of the supervisory guide, provided the position first meets the coverage requirements above based on supervision of non-contractor personnel).

Policy-making or policy-determining functions include responsibility for reviewing staff recommendations on policies developed to affect the organization's mission; considering political, social, economic, technical, and administrative factors with potential impact on recommended policies; and approving those policies.

Distinguishing between SES and SL/ST Positions – Positions that are properly classified above the grade GS-15 grade level, and do **not** meet the functional executive criteria, are more appropriately placed in the Senior Level (SL) or Scientific/Professional (ST) systems. The nature of a position's work determines which system is most appropriate.

• Senior Level (SL) Positions. SL positions are classifiable above the GS-15 grade level, but do not meet the executive criteria characteristic of the SES, nor do they involve the fundamental research and development responsibilities characteristic of ST positions. SL positions may include some supervisory and related managerial duties, provided these duties occupy less than 25 percent of the position's time.

Note: In some instances, the SL system is used for positions that meet the SES executive criteria in agencies that have been excluded from the SES.

• *Scientific/Professional (ST) Positions*. ST positions are classifiable **above the GS-15 grade level** and involve the performance of high-level research and development in the physical, biological, medical, or engineering sciences (or closely related field). ST positions may include some supervisory and related managerial duties, provided these duties occupy less than 25 percent of the position's time. Given the characteristics of project manager work, it is unlikely to occur in ST positions.

6. Designing the Right Position Description

A position description is a statement of the major duties, responsibilities, and supervisory relationships of a given position (<u>http://www.opm.gov/fedclass/gsintro.pdf</u>, p. 11).

The Appendix contains model position descriptions for privacy professionals in different job series. These are closely tied to the draft competency models that map to various sets of privacy requirements, including NIST controls and OMB guidelines.³

Note: Before starting your position design and throughout the process identified in the steps below, you should touch base with your budget and HR offices to ensure your position development activities align with established or emerging conditions. For example, there may be restrictions on budget or the number of available full-time equivalents (FTE) or on hiring generally, changes in processes, or new conditions for employment that may impact your position design, recruitment, or selection process.

Step 1: Consult with your Human Resources Office to identify previously classified position descriptions and other information to use as resources (e.g., job analysis, competency models). Draft and/or update the major duties and responsibilities for the position.

Step 2: Orient the selected model to represent your office, agency and mission with plain language references to relevant offices, their functions, and any relevant administrative notations, such as if the agency is an independent Federal agency. Meet with your HR Office to identify the pay plan, occupational series and title for the position.

Step 3: Describe the position by editing, deleting, and adding descriptive language so that it best represents the position(s) you are designing with the privacy program by employing technically sound position management. Use other resources (e.g., the draft performance competencies, agency studies) to help you determine the balance of functional expertise and capabilities for your position.

Step 4: Engage team members and agency partners in reviewing and commenting on your draft position description. Their input may reveal important job elements that you may not have considered.

Step 5: Consult your HR office to further refine the position description and ensure compliance with HR policies and the inclusion of any necessary language.

The Appendix of this toolkit contains model position descriptions, sample job opportunity announcements and interview questions by job series based on draft competencies.

³ <u>See</u>, <u>e.g.</u>, NIST Spec. Pub. 800-53, Revision 4; OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016); OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (Dec. 2016); OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (Jan. 3, 2017).

III. Recruitment

A. Developing Job Opportunity Announcements

The ability to attract and recruit the best qualified talent to your agency is critical to the success of your agency's mission and the success of the agency's privacy program. Developing a strategic recruitment plan that is tied to the agency's workforce and diversity and inclusion goals will be essential for successful recruitment. This section highlights some areas that will be key in developing a recruitment strategy. Privacy managers should work with agency human resources staff to develop a strategic recruitment plan that best meets the agency's needs.

Any job opportunity announcement (JOA) must include the information required by 5 C.F.R. 330 as described in the <u>Delegated Examining Operations Handbook</u>. It is important to remember that the JOA is also in many cases a chance for the agency to market both the positions and the agency. We recommend that you use the job summary section of the JOA to provide a summary of your agency, its mission, the importance of privacy in the Federal government, and a job summary. Additionally, many agencies have found success in also including links to videos that feature information about the agency or offer a realistic job preview.

Example:

Job Summary

"Privacy has been at the heart of our democracy from its inception." EO 13719. Join the growing cadre of Federal government privacy professionals in ensuring the proper handling of personally identifiable information (PII) and the effective implementation of Federal privacy law and policy. Join the team at the front lines of agency activities in addressing privacy risks that could arise from cutting-edge technologies and addressing complex questions surrounding appropriate collection, maintenance and sharing of PII in an increasingly digital world.

[Brief description of agency's mission.] This position is located in [agency office]. The incumbent reports directly to [manager] and [advises ________ as needed]. The incumbent is responsible for providing support for agency privacy program activities, and will advise, support and assist the agency divisions in their efforts to establish data protection and privacy initiatives, as well as in planning, implementing and assessing privacy program activities.

Example:

Job Summary

Do you desire to protect American interests and secure our Nation while building a meaningful and rewarding career? If so, the Department of Homeland Security (DHS) is calling. DHS components work collectively to prevent terrorism, secure borders, enforce and administer immigration laws, safeguard cyberspace and ensure resilience to disasters. The vitality and magnitude of this mission is achieved by a diverse workforce spanning hundreds of occupations. Make an impact; join DHS.

The primary purpose of this position is to serve as a key advisor to the [supervisor] and other Department officials on issues related to: privacy incident responses, conducting privacy investigations; new and existing privacy policies; advocacy of privacy; and privacy issues presented by new technologies, cybersecurity, and new and proposed legislation; as well as responsible for developing departmental guidance that promotes adherence to the fair information practice principles.

This position is located in the U.S. Department of Homeland Security (DHS), Office of the Secretary and Executive Management, Privacy Office (PRIV).

See the Appendix for sample JOAs by job series.

B. Possible Recruitment Sources

<u>1. Hiring Authorities and Flexibilities</u>

HIRING AUTHORITIES AND FLEXIBILITIES

The Excepted Service

Federal Government civilian positions are generally in the competitive civil service. To obtain a competitive service job, applicants compete with other applicants in open competition. OPM provides excepted service hiring authorities to fill special jobs or to fill any job in unusual or special circumstances under "Schedules A, B, C, and D." These excepted service authorities enable agencies to hire when it is not feasible or not practical to use traditional competitive hiring procedures, and can streamline hiring.

Many excepted service positions are not required to be posted on USAJOBS.gov. Many of the hiring authorities on this list are excepted service authorities.

PATHWAYS PROGRAMS (Schedule D)

The Internship Program

This Program is designed to provide students enrolled in a wide variety of educational institutions, from high school to graduate level, with opportunities to work in agencies and explore Federal careers while still in school and while getting paid for the work performed. Students who successfully complete the program may be eligible for conversion to a permanent job in the civil service.

Who is Eligible:

• Current students enrolled or accepted for enrollment at least half-time in an accredited high school, college (including 4-year colleges/universities, community colleges, and junior colleges); professional, technical, vocational, and trade school; advanced degree programs; or other qualifying educational institution pursuing a qualifying degree or certificate.

The Recent Graduates Program

The Recent Graduates Program affords developmental experiences in the Federal Government intended to promote possible careers in the civil service to individuals who have recently graduated from qualifying educational institutions or programs. To be eligible, applicants must apply within two years of degree or certificate completion (except for veterans precluded from doing so due to their military service obligation, who have up to six years after degree completion to apply). Successful applicants are placed in a dynamic, developmental program with the potential to lead to a civil service career in the Federal Government. The program lasts for 1 year (unless the training requirements of the position warrant a longer and more structured training program).

Who is Eligible:

• Graduates of qualifying educational institutions with an associate's, bachelor's, master's, professional, doctorate, vocational or technical degree or certificate. Individuals must apply within 2 years of degree or certificate completion, except for veterans precluded from doing so due to their military service obligation, who have up to 6 years after degree or certificate completion to apply.

Presidential Management Fellows (PMF) Program

The <u>Presidential Management Fellows (PMF) Program</u> is a flagship leadership development program at the entry-level for advanced degree candidates. Created more than three decades ago, the PMF Program attracts and selects from among the best candidates and is designed to develop a cadre of potential Federal Government leaders. Agency hiring managers may appoint PMF Finalists at the GS-9, GS-11, or GS-12 grade level depending on the Finalist's qualifications. Fellows serve in a two-year excepted service position with the hiring agency, and after successful program completion with good job performance, the PMF may be converted to a permanent position in the competitive service or a term appointment lasting from one to four years, in limited circumstances. The PMF Program is a great way to recruit IT professionals and cybersecurity experts, professors and academics, and other professionals interested in leading, designing, and maintaining a privacy program and gaining valuable experience working on the complex challenges facing the Federal Government. For more information on this program please contact your agency's PMF coordinator.

Who is Eligible:

Individuals who have completed a qualifying advanced degree (e.g., master's degree, Ph.D., J.D.) within the past 2 years; or individuals who expect to complete advanced degree requirements by August 31 of the academic year in which the PMF competition is held.

For More Information on Pathways Programs Visit:

- OPM Website: <u>Hiring Information, Students and Recent Graduates</u>
- Pathways Toolkit for Hiring Managers and Supervisors, A Guide to Hiring Students and Recent Graduates

SCHEDULE A EXCEPTED SERVICE AUTHORITIES ANDDIRECT HIRE AUTHORITIES

Hiring Individuals with Disabilities, Under Schedule A 5 C.F.R. 213.3102(u):

- Under 5 C.F.R. 213.3102(u), Persons with intellectual disabilities, severe physical disabilities, or psychiatric disabilities" can be hired under excepted appointments and also apply under merit promotion job announcements in the Federal government.
- In order to be eligible for employment under this authority, the applicant must provide proof that he/she possesses an intellectual disability, severe physical disability, or psychiatric disability. This documentation must be provided to the hiring agency before an individual can be hired.

•	Documentation of eligibility for employment under Schedule A can be obtained from a licensed medical professional (e.g., a physician or other medical professional certified by a state, the District of Columbia, or a U.S. territory to practice medicine); a licensed vocational rehabilitation specialist (i.e., state or private); or any Federal agency, state agency, or agency of the District of Columbia or a U.S. territory that issues or provides disability benefits.	
•	In addition, upon hiring, the individual with a disability or the agency Human Resource office must complete the <u>Standard Form 256.</u> See OPM Disability Employment for more information, <u>https://www.opm.gov/policy-data-oversight/disability-employment/</u> . An agency may	
	<u>noncompetitively convert</u> to a career or career-conditional appointment in the competitive service an employee who has completed 2 years of satisfactory service under this authority. Satisfactory service is service that begins with a non-temporary (e.g., permanent or indefinite) 5 CFR 213.3102(u) appointment. (Refer to 5 CFR 315.709)	
Hiring GS-905 Attorneys using Schedule A under 5 CFR 213.3102(d)		
•	Attorney positions are in the excepted service and agencies have the authority to establish qualification requirements for their attorney positions. There is no OPM qualification standard for positions in the Attorney positions,GS-0905 series, as OPM is prohibited by law from examining for attorney positions or establishing qualification requirements for them.	
•	Agencies may determine (based on a job analysis) the requirements for their positions	
Hiring Under the Smarter IT Delivery Schedule A Hiring Authority:		
•	In 2015 OPM authorized agencies to use excepted service appointments under 5 C.F.R. 213.3102(i)(3) to address the need for hiring digital services staff to support the President's Smarter IT Delivery Initiative, designed to transform the way the Government builds and procures IT and fundamentally improve the way the Government delivers technology services to the public.	
•	Agencies working on this initiative need staff with skills in modern digital product design, software engineering, product management, creating and maintaining flexible infrastructures, and designing and implementing agile governance structures, all of which require skills and expertise in privacy concepts and requirements, e.g., the ability to design and implement privacy enhancing technologies into digital product design and infrastructure.	
•	Use this authority to fill on a temporary basis for up to one year technical positions needed to carry out the provisions of initiative at the GS-11 through GS-15 levels. Appointments may be extended. See 5 U.S.C. 1302, 3301, 3302, and 5 C.F.R. 213.3102(i)(3) and 302; https://www.chcoc.gov/content/smarter-it-delivery-schedule-hiring-authority.	
Using G	overnment-wide Direct Hire Authority for Information Technology Management (Information	
Security):		
•	Recognizing that the demand for experienced and qualified staff to protect networks and information systems has never been higher, OPM released information in 2015 on hiring flexibilities agencies may use to fill and retain individuals in cybersecurity positions.	
•	Agencies may use direct hire authority to fill positions in Information Technology Management (Information Security and Cybersecurity), GS-2210-09 through GS-2210-15. See 5 U.S.C. 3304(a)(3), 5 C.F.R. Part 337; <u>https://www.opm.gov/policy-data-oversight/hiring-</u>	
•	information/direct-hire-authority/#url=Governmentwide-Authority.	

CYBERCORPS SCHOLARSHIPS FOR SERVICE (SFS) PROGRAM (managed by NSF, in collaboration with OPM and DHS)

What it Provides:

- A way to increase and strengthen the cadre of Federal information assurance professionals that protect the government's critical information infrastructure.
- Scholarships that may fully fund the typical costs incurred by full-time students while attending a participating institution, including tuition and education and related fees. Additionally, participants receive stipends of \$22,500 for undergraduate students and \$34,000 for graduate students. The scholarships are funded through grants awarded by the National Science Foundation.
- Eligible for permanent placement once they complete their obligation.

Who is Eligible:

- Full-time student within two years of graduation with a bachelor's or master's degree; a student within three years of graduation with both the bachelor's and the master's degree; a student participating in a combined bachelor's and master's degree ("five year") program; or a research-based doctoral student within three years of graduation in a coherent formal academic program that is focused on cybersecurity or information assurance at an awardee institution.
- Candidates must be United States citizens, meet criteria for Federal employment; and be able to obtain a security clearance, if required.

How to appoint a candidate:

- Agencies may directly appoint CyberCorps[®] SFS participants into the excepted service and then once they complete their obligation they can be noncompetitively converted to career conditional.
- Use an excepted appointment and cite Section 302 of PL 113-274.

For More Information Visit:

• <u>www.sfs.opm.gov</u>

INTERGOVERNMENTAL PERSONNEL ACT (IPA) MOBILITY PROGRAM

The Intergovernmental Personnel Act Mobility Program provides for the temporary assignment of
personnel between the Federal Government and state and local governments, colleges and
universities, Indian tribal governments, federally funded research and development centers, and
other eligible organizations. An IPA is intended to facilitate cooperation between the Federal
Government and the non-Federal entity through the temporary assignment of skilled personnel.
These assignments allow civilian employees of Federal agencies to serve with eligible non-Federal
organizations for a limited period without loss of employee rights and benefits.

For More Information Visit:

- <u>https://www.opm.gov/policy-data-oversight/hiring-information/intergovernment-personnel-act/#url=Provisions</u>
- <u>https://hru.gov/Studio_Recruitment/HT_05_Intergovernmental_Personnel_Act.aspx</u>

PRESIDENT'S MANAGEMENT COUNCIL INTERAGENCY ROTATION PROGRAM (run by agency Learning and Development offices, managed by OPM)

The PMC Interagency Rotation Program enables emerging Federal leaders at the GS13 to GS-15 levels to expand their leadership competencies, broaden their organizational experiences, and foster networks they can leverage in the future. Specifically, the program aims to:

• Deliver a collaborative, cross-agency program to reduce barriers to interagency mobility.

- Enhance PMC participants' leadership competencies through a meaningful rotational assignment and through other developmental opportunities outside of their current agencies.
- Expand PMC participants' interagency experience either within or outside their current area of expertise.

For More Information Visit:

- <u>https://www.opm.gov/policy-data-oversight/training-and-development/leadership-development/#url=PMC-Interagency-Rotation-Prgm</u>
- <u>https://max.omb.gov/community/display/Management/PMC+Interagency+Rotation+Program</u>

PEACE CORPS AND AMERICORPS VISTA VOLUNTEERS - NONCOMPETITIVE ELIGIBILITY

Individuals who have completed at least one year of Peace Corps service or service with AmeriCorps VISTA are eligible for noncompetitive appointment to the competitive service for 12 months upon successful completion of service. This period of eligibility may be extended for an additional two year due to military service or study at an institution of higher learning.

Individuals who have one year of service with either Peace Corps or VISTA

• <u>See</u> OPM guidance on hiring VISTA alumni and returned Peace Corps volunteers, https://hru.gov/Studio_Recruitment/HT_05_VISTA-Peace_Corps.aspx.

For More Information Visit:

- OPM website, <u>USAJobs, Peace Corps/VISTA Alumni</u>
- Contact your agency's human resources staff.

SHARING CERTIFICATES

Some agencies allow sharing of certifications of candidates between agency offices or components, when the offices or components need to recruit candidates in the same job series and with similar skills. OPM is exploring options for additional sharing of certificates. Ask your Chief Human Capital Officer about whether you may be able to share certificates.

REINSTATEMENT

Agencies may consider filling vacant position(s) with former federal employees who have previously held a career or career-conditional appointment in the competitive service. The reinstatement appointment authority allows current or former Federal employees to re-enter the competitive service. A former federal employee may be appointed under the reinstatement authority within 3 years after the date of separation from their most recent career or career-conditional appointment. There is no time limit on reinstatement eligibility for preference eligibles, or persons who have acquired career tenure by completing 3 years of substantially continuous creditable service. For more information on reinstatement, please review 5 C.F.R. 315.401 or www.opm.gov/policy-data-oversight/hiring-information/reinstatement.

2. Recruitment Resources

RECRUITMENT RESOURCES

USAJOBS.GOV

• Enhance your use of USAJobs and other recruiting mechanisms -- Join USAJobsRecruit, designed to create a Federal recruitment community of practice for sharing best-in-class recruiting practices,

	ideas, insights, and lessons learned, and creating recruiting solutions. <u>https://www.usajobsrecruit.gov/Login/tabid/77/Default.aspx?returnurl=%2fdefault.aspx</u>
•	Try to get your announcement highlighted in the Spotlights area of USAJobs. https://help.usajobs.gov/index.php/Agency_Partners_Functionality_Update
•	Ask points of contact in government to include the USAJobs announcement link in communications to their office or larger community.
FEDER	AL PRIVACY COUNCIL
•	To send your advertisement to over 1000 Federal privacy professionals across the Government, contact the Federal Privacy Council to advertise your position through its privacy jobs email group. See the FPC "Careers" page for contact information and other agency recruiting and hiring resources, <u>www.fpc.gov/careers</u> .
•	Once posted on USAJobs, make sure the position appears in the search results available on the Federal Privacy Council Careers page, <u>www.fpc.gov/careers</u> .
Other	
•	Join multiple social networking sites and post a summary and link to your announcement. Popular sites include: www.linkedin.com/ , http://www.govloop.com/ , http://www.facebook.com/ .
•	Post a summary and link to your announcement on online job boards like <u>www.Monster.com</u> , <u>www.Careerbuilder.com</u> , <u>www.CollegeRecruiter.com</u> , <u>www.TheLadders.com</u> , <u>www.SimplyHired.com</u> , <u>www.LinkUp.com</u> , <u>www.Indeed.com</u> , <u>www.JobCentral.com</u> , <u>www.CareerOneStop.org</u>
•	Contact relevant academic programs and college placement offices, and following their protocol, post a summary and link to your open position or other opportunity.
•	Participate in job fairs held by colleges and universities with degree programs that suit the desired qualifications for your staffing needs. Contact your agency HR representative for more information.
•	Participate in job fairs and job posting services sponsored by organizations with a nexus to performance, such as societies or alumni groups. Contact your agency HR representative to inquire about participating in any job fairs or other recruitment mechanisms sponsored by your agency.
•	Contact academic programs, think tanks or institutes to offer fellowship opportunities to professors or students.
•	Contact continuing education, certificate programs, and organizations that offer learning opportunities, for example, the International Association of Privacy Professionals (IAPP) and American Society of Access Professionals (ASAP).
•	Contact experts in institutes and think tanks, such as Brookings Institution or the Urban Institute, to discuss your needs and ask if they are willing to share your position announcement with promising candidates for advanced analytic staff.
	candidates for davanced analytic start.
IV. Candidate Selection

A. Qualifying and Ranking Applicants

<u>1. Qualifying Applicants</u>

Government-wide minimum qualification standards are published in OPM's **Operating Manual: Qualification Standards for General Schedule Positions**. Most qualification standards permit applicants to qualify on the basis of education/training, experience, or a combination of the two. They include the patterns of education, training, and/or experience most commonly applicable to a particular occupational series. Some qualification standards, however, have specific educational, licensure, or certification requirements that may apply only to specific positions in an occupational series. Agencies and examining offices should select the qualification standard that covers the occupational series to which a position has been classified.

Because privacy work usually requires unique competencies, agencies must determine the paramount knowledge required for occupations that include privacy functions. Once the agency has identified the appropriate occupation for a specific position, the agency can select the proper qualification standard.

The occupational knowledge determines the series of a position for classification purposes (see <u>Determining Occupational Series of Positions with Privacy Work</u>, pp. 10). It also determines the qualifications standard used to screen qualifications of applicants. However, for occupations that involve cybersecurity and privacy work, agencies must include specific cybersecurity competencies to select an individual to fill a position. For minimum qualifications, use the qualification standard appropriate for the occupational series.

Agencies may supplement minimum qualifications with additional KSAs/competencies identified through a job analysis. A job analysis is a systematic method of studying a job to identify the tasks performed and link them to the KSAs/competencies required to perform these tasks. Where appropriate, and supported by a job analysis, agencies may use the competency as a selective factor or quality ranking factor. For additional information on conducting a job analysis and establishing selective and quality ranking factors, agencies may consult <u>OPM's Delegated Examining Operations Handbook</u>.

Selective factors become part of the minimum requirements for a position. A selective factor is a "screen out" (i.e., if an applicant does not meet a selective factor he/she is ineligible for further consideration).

Selective factors:

- Are essential for successful performance on the job (i.e., if individuals do not have the selective factor, they cannot perform the job);
 - For example, a customer service position in an embassy may include a selective factor requiring the employee to speak the language of that country. Or, a posting for a physician may require a medical degree as a selective factor.

- Are almost always geared toward a specific technical KSA/competency;
- Require extensive training or experience to develop; and
- Cannot be learned on the job in a reasonable amount of time.

Selective factors cannot be so narrow that they preclude from consideration applicants who could perform the duties of the position. Agencies may not use selective factors that could be learned readily during the normal period of orientation to the position. Nor should agencies use selective factors that are so agency specific that they exclude from consideration applicants without prior Federal service or preclude selection of applicants from priority placement lists established to assist in the placement of employees affected by reductions in force. Examples of KSAs/competencies that **should not** be used as selective factors include knowledge of:

- An organization's policies and planning processes; and
- An agency's rules, regulations, policies, and guidance.

For additional guidance on developing selective factors please see OPM training "Using Selective Factors".

Note: When using a selective factor, you must specify the required proficiency level.

2. Ranking Qualified Applicants – Quality Ranking Factors

Quality ranking factors are KSAs/competencies that significantly enhance performance in a position, but, unlike selective factors, are not essential for satisfactory performance. Agencies should rank applicants with higher proficiency levels on a quality ranking factor above those with lower proficiency levels. Agencies may not rate qualified candidates ineligible solely for failure to possess a quality ranking factor. With quality ranking factors, the focus is on the level of proficiency the candidate brings to the job. In most Job Opportunity Announcements, the Quality Ranking Factors are expressed in the form of the qualifications questionnaire.

Justification and Documentation: Agencies must document both selective factors and quality ranking factors through job analysis by identifying the:

- KSAs/competencies basic to and essential for satisfactory job performance;
- Duties/tasks the incumbent will perform that require possessing the required KSAs/competencies; and
- Education, experience, or other qualifications that provide evidence of the possession of the required KSAs/competencies.

B. Relevant Educational Backgrounds

<u>1. Privacy Specialist, 0306 Series and Privacy Analyst, 343 Series</u></u>

Privacy work classified to the 0306 and 0343 occupational series do not require positive education. 5 U.S.C. 3308 prohibits OPM and agencies from prescribing minimum education requirements for an

examination unless OPM has determined that the position involves scientific, technical or professional duties that require it. OPM may permit the establishment of minimum educational requirements only when OPM has determined that the work cannot be performed by persons who do not possess the prescribed minimum education. While these positions do not require specialized education, they do involve the type of skills (analytical, research, writing, judgment) typically gained through a college level education, or through progressively responsible experience.

5 U.S.C. 5102(5)(B) requires a link between the level of qualifications required for a job and the level of work as part of the grade level classification process.

As stated previously privacy work can be characterized as multidisciplinary. A multidisciplinary position is a position involving duties and responsibilities closely related to more than one discipline or academic backgrounds. As a result, applicants may qualify for privacy positions based on various educational backgrounds. The nature of the work is such that persons with education and/or experience in either of two or more academic disciplines may be considered well qualified to perform the work.

A job analysis is required for every employment action in the Federal Government (5 C.F.R. 300.103) to validate the competencies required to perform the work of the position.

The following is a list of suggested educational backgrounds, by degree program for undergraduate or graduate work, that could include transferrable knowledge and skills that are useful in performing privacy work:

- Political Science
- Public Policy (general or applied to a particular field such as health)
- Information Management (general or applied to a particular field such as health)
- Law (general or applied to a particular field such as Constitutional Law, Civil Rights and Antidiscrimination Law, Health Law, Consumer Protection, Business and Financial Regulation, Administrative Law and Government Regulation)
- Organizational Sciences and Communications
- Government
- Business
- Health Administration
- Communications
- English
- History
- Public Health
- Political Science
- Philosophy

2. INFOSEC/Privacy Specialist, 2210

The Information Technology 2210 Series includes two options for qualifying applicants. Alternative A covers GS-5 through GS-15 (or equivalent) and must be used for GS-5 and GS-7 positions requiring IT-related education and/or IT-related experience. Alternative B covers only positions at the GS-5 or GS-7 (or equivalent) that do not require IT-related education or IT-related experience upon entry.

Agencies may determine whether to fill their positons via Alternative A or Alternative B. Individuals may qualify based on education and/or experience. This is typical with occupational series are assigned to the Administrative category of work under the General Schedule.

Requirements	
Level	Education
GS-5 (or equivalent)	Bachelor's degree
GS-7 (or equivalent)	1 full year of graduate level education or superior academic achievement
CS 9 (or equivalent)	Master's degree or equivalent graduate degree or 2 full years of progressively higher level graduate education leading to a master's degree or equivalent graduate degree
GS-11 (or equivalent)	Ph.D. or equivalent doctoral degree or 3 full years of progressively higher level graduate education leading to a Ph.D. or equivalent doctoral degree

All OPM Qualification Standards that include positive education require the education be obtained from accredited institutions. The following degrees would be required for the 2210 position:

- Computer Science
- Engineering
- Information Science
- Information Systems Management
- Mathematics
- Operations Research
- Statistics
- Technology Management

To meet this requirement, a candidate also could have another degree, as long as that degree provided a minimum of 24 semester hours in one or more of the above fields and required the development or adaption of applications, systems or networks. This could include the following:

- Cybersecurity
- Identity Management and Security
- Informatics
- Information Assurance⁴

⁴ <u>See</u>, e.g., Colleges with Privacy Curricula, https://iapp.org/resources/article/colleges-with-privacycurricula/.

It would be desirable for candidates with such degrees to have some coursework in privacy. For example, a candidate with an Engineering degree may have taken courses that focus on embedding privacy-enhancing technologies into IT architecture and systems.

3. Attorney 0905 Series

Attorney positions are in the excepted service, and agencies have the authority to establish qualification requirements for their attorney positions. There is no OPM qualification standard for positions in the Attorney, 0905 series, as OPM is prohibited by law from examining for attorney positions or establishing qualification requirements for them.

Agencies may determine based on a job analysis the requirements for their positions, e.g., law degree, J.D. or equivalent, and must be a member in good standing of a state bar, licensed to practice law. Many major law schools in the U.S. now offer a focus in privacy law, which could be desirable for these positions.

Certain undergraduate degrees are also helpful for privacy work:

- Political Science/Law
- Public Policy (general or applied to a particular field such as health)
- History
- English
- Philosophy
- Economics
- For agencies handling PII from outside the U.S., International Relations
- Law (general or applied to a particular field such as Constitutional Law, Privacy Law, Civil Rights and Antidiscrimination Law, Health Law, Consumer Protection, Business and Financial Regulation, Administrative Law and Government Regulation)

4. Continuing Education Courses or Programs

Privacy laws, requirements and best practices are constantly changing. Aside from undergraduate or graduate courses, candidates for a Federal privacy program should regularly participate in continuing education courses or programs, or otherwise demonstrate that they are keeping up with changes in privacy. The following are types of continuing education courses or programs that would be helpful for candidates applying to a privacy program:

- Analytics, Data Analysis
- Communication Complex Information, Plain Language
- Compliance
- E-Government Act
- Emerging Technologies
- Engineering
- Enterprise Architecture
- Federal Information Security Modernization Act

- Freedom of Information Act
- Health Insurance Portability and Accountability Act
- Health Privacy
- Identity and Access Management
- Incident Management
- Information Management
- Information Technology Management
- Outreach and Marketing
- Policy Drafting
- Privacy Act
- Privacy in the U.S. Government
- Privacy in the U.S. Private Sector
- Privacy in Technology
- Privacy Program Management
- Records Management
- Risk Identification and Risk Management
- Security
- Strategic Planning, Strategy Mapping
- System Development and Design
- Training and Education

5. Certifications

OPM has not established certification requirements for the privacy workforce. However, agencies may specify a particular type of certification (or equivalency) in defining quality ranking factors, and for positions in the 2210 series, establishing selective criteria. Subject matter experts must determine that the certification is necessary for satisfactory job performance (i.e., the certification is related to the duties/tasks and required KSAs/competencies of the job). The certification may then be used as evidence validated by a job analysis that a person has the KSAs/competencies needed to perform privacy work at a satisfactory level.

At least three organizations have established robust training programs and also offer certifications or credentials for individuals who pass a test. **Note:** The Federal Government does not endorse or support any of these organizations.

International Association of Privacy Professionals (IAPP), https://iapp.org/:

- IAPP Certification Programs:
 - Certified Information Privacy Professional: U.S. Private Sector (CIPP/US), U.S. Government (CIPP/G), Canada (CIPP/C), Europe (CIPP/E), Asia (CIPP/A)
 - Certified Information Privacy Manager (CIPM)
 - Certified Information Privacy Technologist (CIPT)

American Health Information Management Association (AHIMA), http://www.ahima.org/:

- AHIMA Certification Programs:
 - Certified in Healthcare Privacy and Security (CHPS)
 - Certified Health Data Analyst (CHDA)
 - Certified Healthcare Technology Specialist (CHTS)
 - o Registered Health Information Administrator (RHIA)

(ISC)², <u>https://www.isc2.org/</u>:

- (ISC)² Information Security Certification Programs:
 - Certified Authorization Professional (CAP)
 - Certified Cyber Forensics Professional (CCFP)
 - Certified Cloud Security Professional (CCSP)
 - Certified Information Systems Security Professional (CISSP)
 - Systems Security Certified Practitioner (SSCP)
 - HealthCare Information Security and Privacy Practitioner (HCISPP)

C. Support from Privacy Subject Matter Experts

One consistent problem agencies encounter when recruiting for privacy positions is trying to narrow the pool of applicants to those who are highly qualified and therefore should appear on a certificate of eligible applicants. Privacy is a nuanced multidisciplinary profession, and experience can be gained in multiple fields, including law, policy analysis, information technology disciplines, and even auditing. Thus, identifying relevant experience absent a lengthy narrative can be a challenge for anyone.

Hiring managers <u>can</u> and <u>should</u> be involved in the hiring process to help ensure that the highly qualified applicants appear on the certificate. This includes working closely with HR before the JOA is even posted to:

- ensure the position description is accurate and up-to-date;
- complete a job analysis to identify the critical competencies needed in the job;
- participate in identifying/developing the assessment tool that will be used to evaluate candidates;
- develop a recruiting strategy;
- ensure that the JOA accurately describes the duties of the job, and competencies and experience required in an easy-to-understand and appealing manner; and
- the "qualifications" section of the JOA reflects the top 3-5 skills that an employee must have in order to qualify for the position.

After a JOA is posted and has closed, the next step is to review candidates' applications to determine who is qualified. Unless the individuals conducting this review have significant experience with privacy program work, and understand the skills and experience needed for privacy positions, they may inadvertently place unqualified candidates on the certificate or may omit highly qualified candidates, undermining the selection process. For this reason, privacy hiring managers should consider having someone familiar with privacy conduct the review ("the Subject Matter Expert" review) to determine qualifications. As part of a panel or independently, a privacy

SME will be extremely helpful to a hiring manager and the HR specialist because the SME has experience in identifying the applications of those candidates that have relevant experience that may be difficult for the lay person to understand. For example, a SME might know that a candidate with knowledge of FERPA (the Family Educational Rights and Privacy Act) is equivalent to knowledge of other privacy laws and regulations. The SME also can identify those who may appear qualified but actually have no relevant job experience that aligns to the JOA or position description. The SME can help the HR specialist separate those that have the minimum qualifications and are highly qualified from those who are not qualified. Given the technical nature of privacy positions, agencies should use SMEs as early in the process as possible to ensure that all highly qualified candidates, and only highly qualified candidates, appear on the certificate.

Smaller agencies may have difficulty using SMEs because their privacy programs may not have sufficient staff. Agencies can contact the Federal Privacy Council, <u>www.fpc.gov/Careers</u>, to help identify a SME at another agency, in consultation with the respective Chief Human Capital Officer.

After the applicants are assessed and the referral list is issued, the hiring manager should actively engage in interviewing top candidates and making the selection.

D. Assessment Policy and Tools

Agencies should strive for consistency at each step of the hiring process. Job Opportunity Announcements (JOAs) should link closely to job analyses and position descriptions, and interview questionnaires should address the same competencies laid out in the JOA. OPM provides Federal agencies with assessment policy guidance and tools, i.e., guidance and tools to assist agencies in evaluating candidates' talents and capabilities in the interviewing and hiring process. OPM has developed many online assessment tools – sets of questions for candidates to answer -as part of its Hiring Reform Initiative. They are designed to be used across multiple governmentwide occupations; over time, OPM will evaluate the applicability of the existing online assessments for privacy positions, but agencies may contact OPM to customize assessments for privacy program hiring. See <u>https://www.opm.gov/policy-data-oversight/assessment-andselection/</u>.

The use of effective assessment tools can address barriers to recruiting and hiring privacy talent and improve the quality and diversity of hires, and increase hiring manager satisfaction with the quality of applicants. HR specialists and hiring managers need to collaborate to develop and design effective assessment strategies to hire privacy talent.

All too often, managers do not take the time to review their position descriptions or their Job Opportunity Announcements, and therefore do not end up with candidates that meet their actual criteria. When this occurs, hiring managers may end up selecting candidates based on criteria not reflected in the job announcement. Consistency across the process is key to reducing frustration for applicants and hiring managers. Agencies are encouraged to standardize and document the assessment process through the following steps:

- Ensure that = all individuals are being judged on the same criteria. This is most easily accomplished by adopting a standardized assessment and decision-making process, once which ties directly to the skills needed for the position being filled. "Standardizing" means making a process uniform to ensure the same information is collected on each individual and is used in a consistent manner in employment decisions.
- Once again, consistency starts with all of the skills being reflected equally in each stage of the hiring process. Ensure the selection tool is based on an up-to-date job analysis and is supported by strong validity evidence. A validation study can verify that applicants who score well on the selection device are more likely to do well on the job and contribute to organizational success. Agencies not familiar with validation research methodology are encouraged to consult a measurement expert.

1. Policy

<u>Assessment & Selection Website</u> – contains resources to learn more about personnel assessment, assessment methods, steps to designing effective assessment strategies, and the importance of effective personnel assessment.

Delegated Examining Operations Handbook (DEOH), contains information on the assessment process and policy.

- Chapter 2– Identifying the Job and its Assessments (p. 22);
- **Chapter 5** Assess Applicants (p.90);
- Appendix F Multipurpose Occupational Systems Analysis (p. 233); and
- Appendix G OPM's Job Analysis Methodology (p. 275).

Interagency Assessment Policy Forum – Interagency work group with the focus to improve assessments Governmentwide. Contact OPM at **assessment_information@opm.gov**.

2. Tools

<u>Assessment Decision Tool (ADT)</u> – ADT is OPM's automated system developed to help Federal agencies evaluate and improve their hiring processes to ensure the Federal Government has an effective civilian workforce. The system is designed to help HR specialists and hiring supervisors/managers develop assessment strategies targeted to specific competencies and other situational factors relevant to their hiring situation (e.g., volume of applicants, level of available resources). The ADT is designed to provide you with customized information based on your specific hiring needs.

USA Hire – The USA HireSM assessment battery can be used in conjunction with the traditional occupational questionnaire, and/or additional assessments, such as a Structured Interview, to target agency-specific job requirements. USA HireSM offers the following advantages:

- Objective, professionally-developed assessments
- An efficient and effective tool for evaluating candidates

- Meets all legal guidelines and professional standards
- Applicant friendly
- Ease of implementation as it is already fully integrated with USA Staffing®
- Advanced technology to include computer adaptive testing
- Whole person assessments allow agencies to target critical job-relevant competencies
- More valid measures of applicant competence, reinforced by decades of research supporting the validity of USA HireSM type assessment results

E. General Interview Guidelines for Privacy Positions

<u>1. Pre- Interview: Providing Interviewees with Sufficient Information and</u> <u>Insight</u>

Do not expect candidates to know exactly what your office does or how you do it. It is your responsibility to provide sufficient information – both in writing and verbally – to help the candidate understand more about your office requirements and operations before and during an interview.

Send links to your agency's privacy program web page, System of Records Notices, Privacy Impact Assessments, and web privacy policies, and ask that they familiarize themselves with (not read cover to cover) the work of your office.

Provide an organizational chart and accompanying narrative that clearly shows the position and role of your office in relationship to others.

Briefly describe or summarize the educational and experiential backgrounds of those currently in the office.

Explain what you are looking for in a candidate. This is not giving away the answers you want to hear; this is clearly communicating the factors and needs of the position within your office

Note: Interviews are not 'tests'. They are an opportunity to collaboratively explore the best fit. If you intend to hire anyone you interview, your objective is not to catch them missing the mark (incorrectly guessing what you want them to say) but to mutually explore opportunities and determine where the greatest contributions can be made (a) to your office and (b) to their career development in performance work.

2. Interviews: Possible General Interview Questions

Use a selection of the following general interview questions and the specific privacy questions by occupational series listed above, plus any of your own that are important to the position, to design your own suite of interview questions. They are broken down into three sections:

- a) General questions which are applicable to an entry-level candidate
- b) General questions which are applicable to a mid-career or senior level candidate

c) Specific privacy questions based upon occupational series (0343, 0306, 0905, 2210).

For more information, see **OPM Structured Interview Presentation** - <u>http://www.opm.gov/mediacenter/videos/OPM-Media-Center/Structured-Interview-Training.aspx</u>.

a) General Interview Questions for Interns and Entry-Level Positions

Note: Consider the selection and hiring of an intern or early career employee to be an onboarding experience for them both to Federal service and to Federal privacy program requirements. Do not expect to groom them to stay within your office long-term; it is unlikely that they will. You will instead gain valuable intern/employee contributions to your privacy program and at the same time assist them in developing their career, possibly moving into other Federal offices and positions.

Academic Program and Resulting Knowledge, Skills

Seeking responses that address: analysis of complex issues, without viewing issues in black and white but with nuance and complications that require risk analysis; interest in public policy issues and/or privacy; technical competence; planning and evaluation; reasoning; information management; problem solving; or other competencies important to the position advertised.

- Why did you choose to major in [identify their chosen field of study]?
- Which courses were/are you most drawn to and why? Which course(s) did/do you excel in? Which were/are more challenging?
- We are looking for people with a potential to learn and practice a variety of skills, especially in researching privacy issues, reviewing privacy laws, analyzing requirements, current compliance and developing recommendations to fill any gaps, and drafting privacy-related notices for the public. Of these, tell me/us which is your greatest area of potential and why.

Work Style & Experience

Seeking responses that address: working well with others, collaborating, partnering, influencing and negotiating, conflict management, team building, customer service, interpersonal skills, or other competencies important to the position. Also looking for gaps in resume and experience which could indicate a potential problem.

- Tell me/us about your [part-time, summer, internship, other work experience]? What did/do you think worked/s well about that organization? What would you change?
- Tell me/us about a time when you had to rely on others to get something done that was your responsibility?
- Tell me/us about a time you had to handle a frustrated or angry [internal customer, external customer, or co-worker].
- Tell me/us about a time you were successful in convincing someone to do something they were either reluctant to do, or thought was not a good use of their time.

Career Interests

Seeking responses that address organizational awareness, external awareness, strategic thinking, team building, partnering, influencing and negotiating, accountability, planning and evaluation, information management, public policy and privacy interest, written communication, oral

communication, or other competencies important to the position. See if candidate has dogmatic positions on privacy or is willing to learn, listen and hear all sides of an issue before making a recommendation.

- Why are you interested in this position in the privacy program? What types of privacy issues interest you the most?
- What experience do you wish to gain in this [internship, position] that will help you build your career?
- Tell us about your career progression thus far; please tell us about your career interests.

Federal Government and Your Agency

Seeking responses that address organizational awareness, external awareness, strategic thinking, accountability, planning and evaluation, information management, and other competencies important to the position.

- Why are you interested in a privacy position in our agency?
- (If previous Federal government positions) It seems you enjoy working in the Federal government. Why is that?
- (If no government experience) This would be your first Federal government position. Why are you interested in working in the government?

b) General Interview Questions for Mid- to Senior-Level Candidates

Coaching to Improve Results

Seeking responses that address leadership, collaborative spirit, influencing and negotiating, conflict management, team building, accountability, problem solving, customer service, oral communication, interpersonal skills, or other competencies important to the position.

- Describe a situation in which you collaborated, led, or coached someone or a group of people to achieve a particular goal.
- What have you found to be the most challenging aspect(s) of working with <u>those other</u> <u>staff members?</u> How have you handled the challenge?
- In any privacy program, to achieve its goals, the privacy team must collaborate with other information management type functions, such as information technology, records management, staff in mission-focused offices, and in the Federal government, FOIA. What have you found to be the most challenging aspect(s) of working with other staff members handling other functions? How have you handled the challenge?

Analysis for Decisions and Action

Seeking responses that address privacy analysis, technical competence, planning and evaluation, reasoning, information management, decision making, attention to detail, or other competencies important to the position.

• Describe a recent project that required analysis of a situation.

- What are your strongest <u>analytic skills</u>?
- Describe <u>a situation where your analysis was used</u> to make a significant decision or change a course of action. How did you go about your analysis? How did you present your analysis and conclusions?
- How do you analyze a situation with limited facts?

Reasoning/Critical Thinking/Strategic Thinking

Seeking responses that addresses creativity and innovation, strategic thinking, vision, organizational awareness, problem solving, legal, governance and jurisprudence, compliance, reasoning, decision making, or other competencies important to the position.

- How do you usually <u>approach a problem or challenge</u> when you are working independently? How is your approach different when others are involved?
- What factors need to be considered when <u>reasoning through any government issue</u>? (legal, budgetary, existing legislation, existing guidance, etc.)

Partnering/Team Building/Creating Buy-In

Seeking responses that address vision, leadership, partnering, influencing and negotiating, organizational awareness, team building, political savvy, oral communication, interpersonal skills, or other competencies important to the position.

- How do you/would you go about influencing a person who is not 'sold' on the significance of protecting personal data and privacy rights to actually use it as part of their day-to-day job?
- Describe the challenges and opportunities inherent in partnering across programs within the same department or agency? What about across departments or agencies?
- Describe the challenges and opportunities inherent in cooperating across levels of government and across sectors within the delivery chain of a program such as [insert the title of a key program in your agency and describe it as necessary].
- How do you view conflict? Tell me/us about a conflict that de-escalated or leveraged to produce a better result.

Innovation/Creativity

Seeking responses that address creativity and innovation, external awareness, strategic thinking, vision, change management, flexibility, leadership, problem solving, reasoning, or other competencies important to the position.

• Tell me/us about a recent experience where you used your creativity to design an innovative approach or solution to a problem or challenge?

c) Leadership of Privacy Program, Job Series 306,905 and 2210

Seeking responses that demonstrate leadership, vision, strategic planning experience, resource management and planning, project management, experience comparing program to peer programs, finding creative ways to fill gaps, problem solving, planning and evaluating

- Explain how you would handle strategic planning for an enterprise-wide privacy program?
- In your current privacy program, were there any initiatives that you had hoped to achieve but were unable to achieve, and if so, why?
- Describe two significant accomplishments in leading your current privacy program or implementing initiatives.
- Have you been responsible for programs that did not have sufficient resources to complete all requirements, and if so, how did you manage the workload?
- Have you managed specific projects before, and if so, describe the project, what went well and what you would have improved.

F. Additional Recruiting and Hiring Resources

OPM's Assessment and Selection website includes presentations and tools that agencies may use to develop an assessment strategy and to learn more about various assessment tools and the use of assessments to meet agency specific needs in hiring (e.g., Assessing Students and Recent Grads).

<u>Hiring Toolkit</u> – Provides hiring officials and HR specialists with comprehensive guidance on the Federal hiring process, hiring authorities, assessments, and pay flexibilities.

OPM Cybersecurity Pay and Hiring Authorities – This memorandum provides information on a number of hiring, pay, and leave flexibilities that agencies may use to fill and retain individuals in privacy positions.

If you have questions, contact the appropriate OPM office as follows:

- Classification/Qualifications Policy FedClass@opm.gov
- Assessment Policy Assessment_Information@opm.gov
- Employment or staffing issues Employ@opm.gov
- Pay and Leave Policy pay-leave-policy@opm.gov
- Training and employee development topics HRD@opm.gov

<u>Appendix – Sample Org Structures, PDs, JOAs, Competencies and</u> <u>Interview Questions</u>

This Appendix contains examples of organizational structures for privacy programs, and sample position descriptions (PDs), job opportunity announcements (JOAs), and competencies and interview questions, organized by occupational job series.

Appendix A: Sample Organizational Structures for Federal Privacy Programs

Appendix B: Government Information Specialist (Chief Privacy Officer (CPO) or Privacy Specialist), GS-0306

Appendix C: Program Analyst (CPO, Privacy Analyst or Privacy Program Analyst), GS-0343

Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy Counsel), GS-0905

Appendix E: IT Specialist (CPO, INFOSEC/Privacy Specialist, Privacy Program Manager, or Data Lifecycle Management and Privacy Protection), GS-2210

Appendix A: Sample Organizational Structures for Federal Privacy <u>Programs</u>

Agencies are responsible for managing their resources and deciding how to organize functions and structure positions in a manner that best meets the organization's mission requirements. Following are examples of privacy program organizational structures.

<u>1. Department or Larger Agency</u>



<u>2. Independent or Smaller Agency:</u>



3. Department or Larger Agency (General Counsel as SAOP)



<u>4. Department or Larger Agency (Reporting through CIO)</u>



<u>Appendix B: Samples and Templates for Government Information</u> <u>Specialist (Chief Privacy Officer or Privacy Specialist), GS-0306</u>

<u>1. 0306: Sample Position Description</u>

Government Information Specialist, GS-0306-15 Organizational Title: Chief Privacy Officer Position Description

I. Introduction

[Brief description of agency's mission and privacy program.] This position is located in [agency office]. The Chief Privacy Officer ("CPO") reports directly to the [Agency] Senior Agency Official for Privacy (SAOP), who is accountable for the privacy program. The CPO serves as a senior advisor within the [Agency] for ensuring the consideration and protection of privacy in the collection, maintenance, use, sharing, and disposal of personal information about individuals across all [Agency] programs and activities. The CPO, in developing the [Agency's] privacy program, has the dual role of ensuring [Agency] compliance with privacyrelated laws and also advising other [Agency] Offices and Divisions on privacy-related matters that impact the [Agency's] mission activities and the industry the [Agency] supervises.

II. Major Duties and Responsibilities

Oversees ongoing activities related to the development, implementation, maintenance, measurement of, and adherence to the [Agency's] privacy program including all policies and procedures covering the privacy of personal information and transparency of [Agency's] policies concerning personal information. Develops, implements, and manages policies and controls to sustain compliance with all applicable privacy laws and guidance, including the Privacy Act of 1974, the E-Government Act of 2002, Federal Information Security Modernization Act of 2014 ("FISMA"), and other laws, Executive Orders, court decisions and OMB Guidance. As the agency's recognized privacy subject matter expert, confers technicallysound guidance to senior program management and stakeholders on privacy issues and advises the [Agency head], [Deputy-level], other senior staff, and [Agency] staff concerning privacy policies; legislation, regulations and [Agency] policy initiatives that implicate privacy; novel and complex privacy legal issues; the privacy program; and contracts and data sharing arrangements.

Recognized as the principal privacy advisor throughout the [Agency] and leads crossorganizational teams to identify and mitigate privacy risks. In addition, the CPO develops, implements, and maintains a training and awareness program to educate personnel about **policies and protection of personally identifiable information ("PII"), with the goal of** developing a culture of protection of PII. The CPO will be required to:

- Develop and implement a strategic privacy program plan, with a consistent overall approach to privacy policies and processes, and identification and mitigation of privacy risks.
- Ensure development, implementation and enforcement of privacy-related policies, monitor and measure the effectiveness of the program, benchmark program

components with peer agencies, and regularly improve policies and processes to adapt to best practices, new technologies and issues.

- Monitor, analyze and ensure compliance with privacy laws and requirements, and effectively communicate requirements, risks and recommendations to staff at all levels of [Agency]; analyze current and planned [Agency] policies and activities that may implicate privacy, and assess [Agency] compliance with requirements and advise staff to mitigate risks;
- Establish effective governance over privacy through cross-organizational team(s), including the [relevant information governance or similar teams], charged with identifying and mitigating privacy and security risks, and by establishing the level of privacy responsibility for all [Agency] employees and contractors, including the SAOP, IT policy and compliance staff, staff who handle PII routinely, and all other staff; communicate these roles and responsibilities through policies, procedures, and training and awareness programs.
- Develop privacy workforce planning, supervise and manage the privacy program staff; ensure appropriate skills, training and development for program staff;
- Develop and manages strategic and operational budgets for privacy program, including budget for staff, training, travel, support contractors and service providers, and information technology that may be needed for privacy program operations;
- Develop and implement risk management framework for privacy risks, advise and support staff in mitigating privacy risks and ensuring compliance, particularly with proposed new data collections, throughout the information lifecycle; develop and consider creative solutions to mitigating risks while achieving key mission objectives and working to meet customer expectations;
- Develop and ensure implementation of privacy controls, document such controls, assess the effectiveness of such controls, and in coordination with [Office of Information Technology (OIT)], review each proposed "authority to operate," make recommendations to [Manager/CPO/SAOP] concerning privacy risks and approval, and document plans for strengthening privacy controls as appropriate;
- Develop proposed guidelines or other [Agency] policy statements to enhance data protections and privacy rights of individuals under the organization's authority;
- Develop and maintain inventory of holdings of PII, minimize holdings, regularly review usage of PII within the [Agency], and review disclosures to third parties; work with staff to ensure uses comply with the Privacy Act and privacy notices; for information sharing outside the [Agency], maintain privacy controls through contract or other documentation and reviews of third party handling of PII; develop and implement processes to track disclosures outside the [Agency] according to the Privacy Act;
- Develop and update legally required privacy notices, including system of records notices (SORNs), privacy impact assessments (PIAs), agency privacy policies, and Privacy Act 5 U.S.C. 552a(e)(3) Statements; provide consent as appropriate; and ensure the [Agency] maintains effective access, correction, complaint management, and redress policies and procedures;
- Develop and implement privacy training and awareness plan; develop and deliver privacy training, including training for new staff, annual training and role-based training, and awareness programs, including useful privacy information on the [Agency] intranet site, guest speakers, and newsletters, blogs or other special communications;
- Prepare reports to the Office of Management and Budget, Congress, other oversight bodies and organizations as needed, including but not limited to SAOP FISMA Report;
- Develop and implement technologies, principles and processes to analyze, prioritize and respond to incidents involving loss or unauthorized access to PII; respond to incidents, engage stakeholders to ensure effective response to incidents; maintain

documentation of incidents; and regularly review incidents to understand patterns and develop mitigation measures;

- Keep abreast of proposed and final changes in privacy laws, regulations, guidance, and other requirements;
- Represent the [Agency] privacy office on inter-agency and public/private sector privacy projects, serve on panels and committees to learn and share best practices and support privacy related projects; and support broader Federal privacy community;
- Build coalitions internally on information governance related matters to achieve common goals; actively participate in intra-agency information governance related teams, and collaborate with other members of such teams (e.g., records management, information technology, FOIA, e-discovery) to coordinate requirements and initiatives, and collectively address enterprise-wide information governance problems;
- Ensure compliance with privacy-related issues under the Paperwork Reduction Act;
- Develop and deliver reports and briefings to senior executives, managers and other staff, including on highly sensitive, complex and controversial privacy issues;
- Work with other appropriate divisions of the [Agency] to analyze existing and proposed international data protection and privacy laws, rules, directives, orders and norms for **their impact on the [Agency] mission and to support the [Agency's] enforcement of** privacy-**related laws. Serves as the [Agency's] representative in international data** protection and privacy programs, committees, or organizations.]]

Other duties as assigned.

III. Factor Evaluation Information

Factor 1 – Program Scope and Effect

The Office of Administrative Services, Office of Privacy within the [Agency]. The Office of **Privacy is wholly accountable for the [Agency's] overall** privacy program and ensures compliance with privacy-related statutory, regulatory, and administrative measures.

Factor 2 – Organizational Setting

The incumbent works under the guidance and direction of the Associate Deputy Secretary, Office of Privacy, a Senior Executive Service position.

Factor 3 – Supervisory and Managerial Authority Exercised

The employee exercises delegated authority, oversight, and total management of the Office of Privacy, which includes the Agency Records Division, Privacy Division, and FOIA Division, with approximately eighteen (18) positions, three (3) of which are supervisory, as supportable by the General Schedule Grade Evaluation Guide (GSSG).

Plans work to be accomplished by subordinates, sets and adjusts short-term priorities, and prepares schedules for completion of work; assigns work to subordinates based on priorities, selective consideration of the difficulty and requirements of assignments, and the capabilities of employees; evaluates work performance of subordinates; gives advice, counsel, or instruction to employees on both work and administrative matters; interviews candidates for positions in the unit; recommends appointment, promotion, or reassignment to such positions; hears and resolves complaints from employees, referring group grievances and more serious unresolved complaints to a higher level supervisor or manager; effects minor disciplinary measures, such as warnings and reprimands, recommending other action in more serious cases; identifies developmental and training needs of employees, providing or

arranging for needed development and training; finds ways to improve production or increase the quality of the work directed; and develops performance standards.

In addition to the supervisory responsibilities described above, the incumbent is delegated the supervisory authorities as described below:

- Uses any of the following to direct, coordinate, or oversee work: supervisors, leaders, team chiefs, group coordinators, committee chairs, or comparable personnel; and/or providing similar oversight of contractors.
- Exercises significant responsibilities in dealing with officials of other offices or organizations, or in advising management senior officials.
- Assures reasonable equity (among groups, teams, projects, etc.) of performance standards and rating techniques developed by subordinates or assuring comparable equity in the assessment by subordinates of the adequacy of contractor capabilities or of contractor completed work.
- Makes decisions on work problems presented by subordinate supervisors, team leaders, or similar personnel, or by contractors.
- Evaluates subordinate supervisors or leaders and serving as the reviewing official on evaluations of nonsupervisory employees rated by subordinate supervisors.
- Makes or approves selections for subordinate nonsupervisory positions.
- Recommends selections for subordinate supervisory positions and for work leader, group leader, or project director positions responsible for coordinating the work of others, and similar positions.
- Hears and resolves group grievances or serious employee complaints.

Factor 4 – Personal Contacts

Subfactor 4A – Nature of Contacts

The employee interacts on a daily basis with persons representing organizations or groups from inside and outside the Office of Administrative Service and the Department. This includes senior leadership, senior officials within the Office of the Chief Information Officer and across the Department, program management specialists, consultants, vendors, and contractor personnel. Person-to-person work relationships involve technical discussions, recommendations, and decisions of high order. Contacts take place at meetings, conferences, briefings, speeches, lectures, presentations, seminars, etc.

Subfactor 4B – Purpose of Contacts

The employee provides authoritative advice and coordination to justify, influence, motivate, or settle matters involving privacy programs and policies. The employee represents the bureau/office as technical advisor, coordinating and information gathering, resolving privacy requests or complaints, explaining privacy programs and policies, or facilitating the building of consensus positions on issues from several divergent and conflicting advocates or groups.

Factor 5 – Difficulty of Typical Work Directed

The incumbent will be involved in planning, operations, studies, and analyses that are significant to the bureau/office as well as the Department. The incumbent advises leadership on privacy issues and activities, and develops and implements bureau-wide policies for effective management of the privacy program. Results of the work are mission critical. The incumbent performs assignments characterized by substantial intensity, highly technical complexity, many interrelationships, complex operations and variables, and new approaches and methodologies. Multiple parallel assignments are usually in progress, many without

precedent and of varying durations. The incumbent must have the skill to plan, organize, and direct operations and studies, and understand the direction and vision of the Associate Deputy Secretary, as well as privacy policies and directives. In-depth analysis, extensive coordination, and recommendations with different high level officials are required to meet mission requirements. The GS-14 grade represents the highest grade which best characterizes the nature of the basic mission-oriented nonsupervisory work performed within the bureau/office, and constitutes at least 25% of the workload of the core.

Factor 6 – Other Conditions

Supervision and oversight at this level requires exceptional coordination and integration of a number of very important and complex program segments of technical, managerial, or administrative work comparable in difficulty to the GS-14 grade.

2. 0306: Sample Job Announcement

0306 - 15 Job Opportunity Announcement

Agency: [Insert name and logo]

Job Announcement Number: [Insert number]

CHIEF PRIVACY OFFICER, GS-0306-15

SALARY RANGE: \$XX,XXX - \$XX,XXX USD per year	OPEN PERIOD: [Insert Opening to Closing Dates]
SERIES & GRADE: GS-0306-15	POSITION INFORMATION: [Full- time/Permanent or Term as determined by agency]
PROMOTION POTENTIAL: [As determined by agency]	LOCATIONS: [Insert Duty Location(s)]
WHO MAY BE CONSIDERED: United States Citizens	[If you identify your targeted applicant pool(s) in the Job Builder template, Career Patterns icons will be automatically inserted here, e.g., Time in Career, Mobility, etc.]

Job Summary:

[Insert agency logo, optional]

[Insert information to attract your targeted talent pool(s) including agency's

branding/marketing/mission and work environment aspects e.g. telework, work schedules and other flexibilities. For help, go to <u>https://www.opm.gov/policy-data-oversight/human-</u> <u>capital-management/#url=Framework</u>.]

Please see the sample language below.

Do you desire to protect American interests and secure our Nation while building a meaningful and rewarding career? If so, the [Agency] has the job for you.

In this role the Chief Privacy Officer serves as a senior advisor within the [Agency] for ensuring the consideration and protection of privacy in the collection, maintenance, use, sharing, and disposal of personal information about individuals across all [Agency] programs and activities.

Great Benefits Package: paid vacation, sick days, holidays, health and life insurance, and an excellent retirement package!

Key Requirements:

- U.S. Citizenship or National
- Registered for Selective Service, if applicable (See <u>Other Information</u>)
- Meet specialized experience requirements (See <u>Qualifications and Evaluations</u>)
- Résumé and supporting documents (See How to Apply)
- Complete the <u>Occupational Questionnaire</u>
- Suitable for Federal employment

The CPO will oversee ongoing activities related to the development, implementation, maintenance, measurement of, and adherence to the [Agency's] privacy program including all policies and procedures covering the privacy of personal information and transparency of [Agency's] policies concerning personal information. Develops, implements, and manages policies and controls to sustain compliance with all applicable privacy laws and guidance, including the Privacy Act of 1974, the e-Government Act of 2002, Federal Information Security Modernization Act ("FISMA"), NIST privacy-related controls, and other laws, Executive Orders, court decisions and OMB Guidance. As the agency's recognized privacy subject matter expert, confers technically-sound guidance to senior program management and stakeholders on privacy issues and advises the [Agency head], [Deputy-level], other senior staff, and [Agency] staff concerning privacy policies; legislation, regulations and [Agency] policy initiatives that implicate privacy; novel and complex privacy legal issues; the privacy program; and contracts and data sharing arrangements. The CPO will:

- Lead cross-organizational teams to identify and mitigate privacy risks.
- Develop, implement, and maintain a training and awareness program to educate personnel about policies and protection of personally **identifiable information ("PII")** to work toward developing a culture of protection of PII.
- Develop and implement a strategic privacy program plan, with a consistent overall approach to privacy policies and processes, and identification and mitigation of privacy risks.
- Ensure regular enforcement of privacy policies, monitor and measure the effectiveness of the program, benchmark program components with peer agencies, and regularly improve policies and processes to adapt to best practices, new technologies and issues.
- Establish effective governance over privacy through cross-organizational team(s), including the [relevant information governance or similar teams], charged with identifying and mitigating privacy and security risks, and by establishing the level of privacy responsibility for all [Agency]

employees and contractors, including the SAOP, IT policy and compliance staff, staff who handle PII routinely, and all other staff; communicate these roles and responsibilities through policies, procedures, and training and awareness programs.

- Supervise and manage the privacy program staff; ensure appropriate skills, training and development for staff.
- Develop and manage strategic and operational budgets for privacy program, including budget for staff, training, travel, support contractors and service providers, and information technology that may be needed for privacy program operations.
- Develop and implement risk management framework for privacy risks, advise and support staff in mitigating privacy risks and ensuring compliance; develop and consider creative solutions to mitigating risks while achieving key mission objectives and working to meet customer expectations.
- Develop and ensure implementation of privacy controls, document such controls, assess the effectiveness of such controls, and in coordination with [Office of Information Technology (OIT)], review each proposed "authority to operate," make recommendations to [Manager/CPO/SAOP] concerning privacy risks and approval, and document plans for strengthening privacy controls as appropriate.
- Develop and maintain inventory of holdings of PII, minimize holdings, regularly review usage of PII within the [Agency], and review disclosures to third parties; work with staff to ensure uses comply with the Privacy Act and privacy notices; for information sharing outside the [Agency], maintain privacy controls through contract documentations and reviews of third party handling of PII; develop and implement processes to track disclosures outside the [Agency] according to the Privacy Act.
- Develop and update legally required privacy notices, including system of records notices (SORNs), privacy impact assessments (PIAs), agency privacy policies, and Privacy Act 5 U.S.C. 552a(e)(3) notices; provide consent as appropriate; and ensure the [Agency] maintains effective access, correction, complaint management, and redress policies and procedures.
- Develop proposed rulemakings, guidelines or other [Agency] policy statements to enhance data protections and privacy rights of individuals whose activities are regulated by the [Agency].
- Build coalitions internally on information governance related matters to achieve common goals; actively participate in intra-agency information governance related teams, and collaborate with other members of such teams (e.g., records management, information technology, FOIA, ediscovery) to coordinate requirements and initiatives, and collectively address enterprise-wide information governance problems;
- Ensure compliance with the privacy-related provisions of the Paperwork Reduction Act.
- Prepare reports to the Office of Management and Budget, Congress, other oversight body and organizations as needed, including but not limited to SAOP FISMA Report.
- Develop and implement technologies, principles and processes to analyze, prioritize and respond to incidents involving loss or unauthorized access to PII; respond to incidents, engage stakeholders to ensure effective response to incidents; maintain documentation of incidents; and regularly review incidents to understand patterns and develop mitigation measures.
- Work with other appropriate divisions of the [Agency] to analyze proposed international data
 protection and privacy laws, rules, directives, orders, etc. for their impact on the [Agency] mission
 and to support the [Agency's] enforcement of privacy-related laws.

Qualifications and Evaluation

Qualifications Required:

GS-15: You qualify at the GS-15 level if you possess one (1) year of specialized experience, equivalent to at least the GS-14 level in the Federal Government, which has equipped you with the skills needed to successfully perform the duties of the position. You must have experience performing the following duties:

Have at least 1 full year of specialized experience equivalent to the GS-14 level in the Federal service which provided you with the particular knowledge, skills and abilities to perform the duties of the position Qualifying specialized experience must demonstrate the following:

- Serving as a Program Manger within the Privacy Program, providing technical and administrative supervision covering privacy laws, policies, safeguards, business processes and initiatives and representing [Agency] on a wide variety of privacy issues and policies;
- Exercising agency responsibility for overseeing release of, or access to, [Agency] records, record systems, and complying with Federal laws and [Agency] policies and directives concerning the maintenance, access and release/non-release of personally identifiable information (PII);
- Formulating, developing and implementing initiatives that include oversight of the collection, use, and dissemination of PII; ensuring that sufficient technical and administrative measures are implemented to ensure the security of [Agency] data systems, processes, and facilities;
- Communicating privacy initiatives with a variety of internal and external constituents, including the media, in coordination with the Office of Public Affairs and the [Agency].

[Agency must define specialized experience].

Your education, training, and/or experience must show that you possess the following competencies

- Privacy Technical Competencies
- Leadership
- Program Management
- Written Communication
- Oral Communication

How You Will Be Evaluated:

We will review your résumé to ensure you meet the basic qualification requirements. Applicants meeting basic qualification requirements will further be evaluated on the information provided in the Occupational <u>Questionnaire</u>. The <u>Occupational Questionnaire</u> collects information on your education, training, and experience related to critical competencies, such as project management, writing, oral communication, influencing/negotiating, problem solving, and attention to detail. [Insert Agency Evaluation Procedure].

Benefits and Other Information

Benefits and Other Information:

Benefits:

Working for [Insert agency name] offers a comprehensive benefits package that includes, in part, paid vacation, sick leave, holidays, life insurance, health benefits, and participation in the Federal Employees Retirement System. [Insert agency specific benefits/flexibilities that may be

attractive to potential applicants identified in your Career Patterns analysis, e.g., telework options, recruitment or relocation incentives, flexible work schedule, etc.] The following Web address is provided for your reference to explore the major benefits offered to most Federal employees. To find out more click here http://www.usajobs.opm.gov/ei61.asp.

Other Information:

Interagency Career Transition Assistance Program (ICTAP). The ICTAP provides eligible displaced Federal competitive service employees with selection priority over other candidates for competitive service vacancies. If your agency has notified you in writing that you are a displaced employee eligible for ICTAP consideration, you may receive selection priority if this vacancy is within your ICTAP eligibility, you apply under the instructions in this announcement, and you are found well-qualified for this vacancy. **[Insert agency definition of well-qualified.]** You must provide proof of eligibility with your application to receive selection priority. Such proof may include a copy of your written notification of ICTAP eligibility or a copy of your separation personnel action form. Information about ICTAP eligibility is on OPM's Career Transition Resources website at http://www.opm.gov/ctap/index.asp.

[Insert the following paragraph if your agency did not clear CTAP before announcing outside its own workforce.]

Career Transition Assistance Plan (CTAP). The CTAP provides eligible surplus and displaced Federal competitive service employees with selection priority over other candidates for competitive service vacancies. If your agency has notified you in writing that you are a surplus or displaced employee eligible for CTAP consideration, you may receive selection priority if this vacancy is within your CTAP eligibility, you apply under the instructions in this announcement, and you are found well-qualified for this vacancy. [Insert agency definition of well-qualified.] You must provide a copy of your written notification of CTAP eligibility with your application. Information about CTAP eligibility is on OPM's Career Transition Resources website at http://www.opm.gov/ctap/index.asp.

Selective Service: If you are a male applicant born after December 31, 1959, you must certify that you have registered with the Selective Service System, or are exempt from having to do so under the Selective Service Law. See <u>www.sss.gov</u>.

Veterans' Preference: If you are entitled to veterans' preference, you should indicate the type of veterans' preference you are claiming on your résumé. Your veterans' preference entitlement will be verified by the employing agency.

- For 5-point veterans' preference, please provide your DD-214 (Certificate of Release or Discharge from Active Duty), official statement of service from your command if you are currently on active duty, or other official documentation (e.g., documentation of receipt of a campaign badge or expeditionary medal) that proves your military service was performed under honorable conditions.
- For 10-point veterans' preference, please submit a <u>Standard Form (SF) 15</u>, *Application for 10-Point Veteran Preference* and the required documentation.

How To Apply:	
APPLY ONLINE	

Federal Privacy Council / OPM

You may either 1) or 2) deliver your application package via [Insert agency procedure.] Your complete application package will include:

- 1. Résumé
- 2. Occupational questionnaire
 - If you are applying online, <u>click here</u> to complete the Occupational Questionnaire
 - If you are NOT applying online,
 - i. <u>click here</u> to download the Occupational Questionnaire
 - ii. <u>click here</u> to download the form you must record your responses on

If faxing in your application package: Attention: [Insert name of contact] [Insert telephone number]

Send Mail

[Insert complete address] USA

All electronic submissions or faxes must be submitted and received by [Insert time] Eastern Time [Insert closing date.] All mailed résumés and/or supporting documents must be received by [Insert closing date.] [Insert agency application receipt procedures if different.]

What to Expect After You Apply:

After all application packages have been received, we will review your résumé to ensure you meet the basic qualification requirements. We will evaluate each applicant who meets the basic qualifications on the information provided in the <u>Occupational Ouestionnaire</u> and may interview the best-qualified applicants. After making a tentative job offer, we will conduct a suitability and/or security background investigation. A final job offer for this position is typically made within 40 days after the deadline for applications.



[Insert name of contact] Phone: **[Insert contact's phone number including area code]** TDD: [Insert TDD phone number including area code] Email: **[Insert contact's email address]**

EEO Policy Statement

The United States Government does not discriminate in employment on the basis of race, color, religion, sex, national origin, political affiliation, sexual orientation, marital status, disability, age, membership in an employee organization, or other non-merit factor.

Reasonable Accommodation Policy Statement

Federal agencies must provide reasonable accommodation to applicants with disabilities where appropriate. Applicants requiring reasonable accommodation for any part of the application and hiring process should contact the hiring agency directly. Determinations on requests for reasonable accommodation will be made on a case-by-case basis.



USAJOBS Control Number: [Insert number]



3. 0306: Sample Competencies and Interview Questions

0306 Sample Interview Questions

The interview questions below are categorized by some of the high-level general or technical competencies needed for positions in this job series, with some examples of more specific competencies that are also addressed. This list of competencies is not a complete, exhaustive list. Also, some questions address more than one competency – some address many competencies—while others may only address one specific competency. These questions are intended to be a useful starting point for you to develop specific questions for a position. **Note**: The interviewer should explain to the applicant that, while the questions ask for examples and work experience, the applicant should not reveal any information that is sensitive or confidential to another organization.

Disclosure: A competency study will be completed to validate the competencies included in this toolkit and needed to perform privacy work government-wide. Also, please note that Federal regulations (5 C.F.R. Part 300.103) require that each employment practice be based on a job analysis. A job analysis must be completed to validate the competencies used to evaluate applicants for Federal positions.

Competencies, 0306	Questions
Analytical Reasoning	Q: How do you define privacy? What do you see as the biggest challenges to privacy protection today?
	Q: Why is privacy important for the government to maintain the public trust?
Interpersonal Skills	Q: Please describe at least two situations where you worked on a
Includes Teamwork, Conflict Management, Influencing/Negotiating	team. What role did you have on the team, what went well, what were the challenges, and did the team accomplish its goals?
Compliance Includes Authority to Collect, Purpose	Q: Please describe any processes or policies you have used or would recommend to ensure that your organization has authority to collect new data types.
Specification, Accounting of Disclosures, Regulations and Policy, Accountability	Q: If a person sent an email to your organization that contained sensitive PII, but was not requested, does the organization have a privacy obligation to protect it, legal or otherwise? What actions should be taken?
	Q: Please describe any experience you have had with procedures or processes to track disclosures (as required by the Privacy Act).
	Q: How has your organization planned (is your organization planning) to implement revised OMB Circular A-130? What will be the most significant changes for how your program has been operating?
Transparency	Q: What do you think about website privacy policies? Are they useful?
Includes Transparency,	What should they cover? Why?

Competencies, 0306	Questions
<i>System of Records Notices and Privacy Act Statements</i>	Q: What is a System of Records Notice (SORN), and why is a SORN important for the privacy program? Q: What law mandates that a SORN be created, and how is the SORN communicated to the public?
	Q: What are the main challenges to effective mobile phone disclosures?
Individual Participation and Redress Includes Consent, Individual Access, Correction and Redress, Complaint Management	 Q: What do you view as the most effective ways to achieve consent to the handling and disclosure of PII? Do you see any challenges with how consent is handled with evolving technologies? What are some public considerations related to obtaining an individual's consent to use and/or disclose his or her PII? Q: How would you advise a program office that is planning to use an individual's PII for purposes other than originally stated in their public notices?
	Q: Please describe any experience you have had responding to Privacy Act requests for access, correction or redress.
	Q: If you were to receive a call or email from a member of the public with a privacy concern, what steps would you take to address the issue?
Minimization	Q: Does your agency define "sensitive PII," and if so, how and why?
Includes Minimization of PII, Minimization of PII Used in Testing, Training and	Q: Does your agency have a "PII inventory," and if so, please describe your involvement or experience working with it. How it was developed and how it is regularly maintained?
Research, and Data Retention and Disposal,	Q: Please describe efforts you have taken in your work to minimize collection and retention of PII.
Inventory of Personally Identifiable Information	Q: What questions or issues would you raise with a person who brings you a project that would involve collection and processing of sensitive PII?
	Q: What is the value of an inventory of personally identifiable information? Please explain how you have helped develop or maintain such an inventory.
	Q: What is anonymizing data, and how does that differ from de- identifying data? How would you guide an organization in anonymizing or de-identifying data it plans to share with a third party?
Use Limitation Includes Internal Use	Q: Describe how you have interpreted the requirements to share information internally only with those who "need to know" the information, and the processes put in place to implement this requirement.
	Q: What measures can an organization take to help ensure that PII is only shared externally as authorized?

Data Quality and Integrity	Q: What are some ways an organization can help ensure data quality and integrity?
Policy Analysis and Development	Q: What are some of the most effective privacy or security policies you have read? What elements made them effective?
Includes Monitor and Analyze Privacy Law and Policies	Q: Explain the difference between answering a question with "what is legally acceptable" vs. "what is the right thing to do?" Have you faced this question in your work?
	Q: Describe privacy-related policies you have drafted or had input into, and any challenges you faced in drafting, organizational adoption of the policy, or implementation.
	Q: Have you followed proposed laws or amendments to laws that may impact your organization? Which laws and what types of impact did you recognize?
	Q: [If agency collects and maintains data from the EU] Please explain your familiarity if any with the EU General Data Protection Regulation (GDPR). If familiar with the GDPR, what do you see as the most significant impacts of the GDPR on U.S. organizations, public and private sector?
	Q: [If agency collects and maintains data from the EU] What is your organization's legal basis for transferring personal data from the EU to the US, and how might that change under the GDPR?
Privacy Advice and Guidance	Q: Your responsibility includes supporting the organization's business operations by advising on privacy requirements. Explain scenarios where you have advised other employees on privacy requirements, your approach, what worked well, and what challenges you faced.
	Q: How do you measure the success of a privacy program/policy? What metrics might be important to collect and review?
	Q: Tell me about a time you influenced others to re-think a business approach because it raised significant privacy risks.
Privacy Awareness and	Q: Describe situations where you have had to train other individuals.
Training	Q: How are your organization's training programs handled, and what are the key topics in those programs?
	Q: What has been your most effective staff awareness activity?
	Q: In addition to annual training, what other types of privacy training does your organization provide and how are you involved?
	Q: <i>[mid to senior level positions]</i> Describe the types of activities you have led on Data Privacy Day.
	Q: <i>[senior level position]</i> Describe the types of privacy training you have delivered, the audience for that training, and any reactions or outcomes you recall from the training.
	Q: [mid to senior level position] What format of training have you found to be most effective?

Continual Learning (General Competency)	Q: How do you keep up with changes to privacy laws, policies and standards?
	Q: What was the last training or privacy program you attended?
Privacy Impact and Risk Assessment Includes Privacy Risk Management/ATOs, Privacy	Q: If an employee brought to you a project involving collection of new types of sensitive PII, where would you start in analyzing the project and providing guidance? What protections would you want in place and why?
Risk Management	Q: What do you think are the top three privacy risks in most Federal Government agencies?
	Q: What is a Privacy Impact Assessment (PIA) and when should a PIA be performed?
	Q: What are the benefits of a privacy specialist reviewing and approving a PIA, rather than arranging for the IT group by itself to review and approve a PIA?
	Q: Please explain some of the types of risks you have identified in conducting PIAs and how you have mitigated those risks.
	Q. Provide examples of the privacy controls described in NIST Spec. Pub. 800-53, Revision 4, and tell us your experience in developing, implementing and assessing the effectiveness of privacy controls.
	Q: What do you see as differences between information security and privacy? And how are they aligned?
	Q: How have you, or would you, implement "privacy by design" (PbD)? How would you gain access to the system developers to influence them to adopt PbD standards in the system development lifecycle? What obstacles have you encountered in implementing PbD?
Privacy Incident Response Includes Incident	Q. In your own words, what is a PII data breach and, as the privacy specialist, what would you want to know about such a breach?
Management	Q: Have you ever been involved in helping respond to a breach of personal data or other data security incident? Describe your experience and role, if any, in investigating the breach or other incident, providing notice to affected individuals, determining what steps should be taken to mitigate the breach or incident, developing strategies for avoiding similar breaches or incidents in the future, and other lessons learned.
	Q: What is the importance of notification of affected individuals when data breaches occur?
	Q: Explain any experience you have had in notifying appropriate government authorities about a data breach.
Information Sharing With Third Parties Includes Privacy	Q: Describe your experience with retaining and using contractors that handle or process PII, or if you have not had this experience, what issues you would expect to address. What actions have you taken, or
Requirements for Contractors and Service	would you take, to ensure that PII is sufficiently protected? Q: How would you assess third parties who handle PII on the
	a. now would you docoo third parties who handle i if on the

Providers, Contract and Grant Oversight	organization's behalf?Q: Describe ways that you could assure yourself that a service provider is actually doing what it says it is doing.Q: Does your organization use cloud technology, if so, how are any privacy concerns addressed?
Privacy Reporting	Q: Have you participated in providing written reports to your senior staff, Congress, OMB or other government agencies (or if private sector, your Board of Directors)?
	Q: [mid to senior level] Please describe the types of briefings or presentations you have provided to your senior staff, Congress, or others (or if privacy sector, Board of Directors).
	Q. What is FISMA and how does FISMA apply to your agency's privacy program?
Project Management	Q: Describe situations where you have managed projects. What went well, what were the challenges, and did you accomplish your goals?
Privacy Monitoring and Auditing	 Q: How would you address gaps in privacy processes within an organization? Q: You have been tasked to conduct a privacy compliance review and present recommendations about how PII is handled. The organization is led by a senior executive who collects sensitive information from and about the public. You believe there is room for improvement in how the information is collected, managed, accounted for and secured. How would you approach this project in terms of tasks and major considerations?
Senior Level Positions: Governance and Privacy Program Includes Program Management, Developing Others, Leadership	 Q: What are some of the primary responsibilities of an organization's privacy program? Q: What do you view as the most effective organizational governance structure of a privacy program within an organization, e.g., reporting relationships? Q: Please describe your experience developing and implementing budgets. What key lessons have you learned from your experience? Q: Privacy leaders often dream of implementing the ideal privacy program, but the reality is often that the resources are not available. How would you manage a privacy program to make the most of the resources you have?
Supervisory Positions: Workforce Planning Includes Managing Human Resources, Developing Others, Employee Development	 Q: Explain your experience in workforce planning. Are you familiar with the parts of OMB revised Circular A-130 regarding workforce planning, and if so, how would you meet those requirements? Q: Please describe your experience managing other employees, including how you have developed employees. Q: What key lessons have you learned in your experience as a manager?

<u>Appendix C: Program Analyst (CPO, Privacy Analyst or Privacy</u> <u>Program Analyst), GS-0343</u>

<u>1. 0343: Sample Position Description</u>

OFFICIAL TITLE: Program Analyst, GS-0343-13

ORGANIZATIONAL TITLE: Privacy Analyst, GS-0343-13

Position Description

INTRODUCTION

The Privacy Division has oversight responsibility for the [Agency] Privacy Program. The Division determines and provides [Agency] wide policy guidance as it pertains to the overall conduct of the Program. The Division is guided by internal agency directives, the Privacy Act or 1974 (as amended), Section 803 of Public Law 110-53 (Implementing Recommendations of the 9/11 Commission Act of 2007), portions of the Federal Information Security Modernization Act (FISMA), the E-Government Act, and various Office of Management and Budget (OMB) circulars and memoranda, and NIST security and privacy controls. The Division directly supports the Senior Agency Official for Privacy (SAOP) for the [Agency].

DUTIES:

The incumbent of this position serves as a management analyst on the staff of the Privacy Division with primary responsibility for advising management on the effectiveness of the [Agency] privacy program, researching new practices to improve effectiveness, overseeing [Agency] Component compliance with statutory and regulatory requirements related to the establishment and revision of Privacy Act systems of record notices (SORNs), the creation of Privacy Act procedural and exemption rules under the Administrative Procedures Act, the development and coordination of Privacy Act Computer Matching Agreements (CMAs), and the reporting and tracking of privacy incidents. The incumbent also supports oversight and management of other privacy compliance and risk management efforts. In addition, the incumbent will lead implementation of privacy program compliance activities. The incumbent will:

- Analyze and evaluate the effectiveness of the privacy program in meeting its requirements and objectives;
- Research and investigate new or improved business and management practices to strengthen the privacy program;
- Analyze new or proposed legislation or regulations to determine impact on program operations and management and ensure [Agency] Privacy Program compliance.
- Assess key business objectives, new product development concepts, proposed information collections and technology changes, and marketing initiatives being undertaken by [Agency offices] to develop and ensure implementation of privacy controls, and ensure appropriate authority to collect and data minimization.
- Ensure [Agency] use of appropriate privacy notices, e.g., SORNs, privacy impact assessments and privacy policies.

- Plan, develop, and deliver [Agency] wide privacy training materials for [Agency] Components. Training materials serve as a basis for providing training to agency personnel or as a template for the development of specialized training to be provided by the [Agency] Components.
- Provide training or briefings to [Agency] Component privacy officers and their staff for in-person/webinar/video-teleconference venues.
- Ensure accurate and timely information is posted to the [Agency] Privacy Office website and SharePoint site.
- The incumbent participates in special projects and initiatives and performs special assignments. Identifies the need for special projects and initiates milestones and goals.
- Evaluate reports by analyzing facts and performing appropriate research and prepare detailed responses.
- Determine appropriate recommendations for unresolved or questionable problems and perform follow-up.
- Research and determine or recommend appropriate actions or interpretation of issues impacting the serviced organizations.
- Represent [Agency] with a variety of organizations.
- Establish, develop, and maintain effective working relationships with customers; meet with key customer and coordinating officials to assess customer satisfaction, explain policy and procedures, and resolve problems.
- Provide or ensure subordinates provide customer guidance and training.
- Research and determine or recommend appropriate actions or interpretation of issues impacting the organization or agency.
- Prepare and present high-level briefings; prepare and analyze reports; respond to queries, justifications, and background papers on areas of expertise and assignment.
- Research and determine or recommend appropriate actions or interpretation of issues impacting the organization.
- At times, serve as the independent technical authority for the organization.
- Represent the organization on working groups; steering groups; or other meetings, conferences, seminars, etc. May chair such groups or meetings when the meeting is in the incumbents area of assignment.
- Promote interchange of information on Privacy requirements, capabilities, deficiencies, and technology applications.
- Defend recommendations to higher levels of management as necessary.

CLASSICATION CRITERIA

Factor 1, Knowledge Required By The Position Level 1-8 1550 Points

Mastery of advanced management and organizational principles and practices, and extensive knowledge sufficient to plan, organize, direct, and evaluate a comprehensive privacy review, analysis, and internal control operation, together with the skills to successfully implement the program at the Department and Component level.

Thorough knowledge of the Privacy Act of 1974 and related laws and regulations, Federal and Department privacy policies and practices to advise [Agency] Component Privacy Officers, program managers, and agency counsel and to provide guidance and assistance relating to organizational privacy requirements, reviews, and analysis.

Knowledge of [Agency] missions, programs, and organizational relationships and program goals and objectives, the sequence and timing of key operational events and milestones, and
methods of evaluating the effectiveness of planning actions as related to actual events i.e., privacy incidents.

Ability to communicate and relate effectively with [Agency] Component Privacy Officers, program managers, agency counsel and employees at all levels of the organization in order to ensure that statutory and regulatory privacy requirements are appropriately coordinated and incorporated into pertinent organizational directives, policies, and practices.

Skill in designing and conducting comprehensive studies, and developing solutions to broad, important, and severe operational and privacy areas.

Ability to plan, organize, and develop studies or projects, and to negotiate effectively with management to accept and implement recommendations, where the proposals involve substantial resources, and require extensive changes in established concepts and procedures.

Factor 2, Supervisory Controls Level 2-4 450 Points

Supervisor and employee develop a mutually acceptable project or study plan, which includes identification of the work to be done, the scope of the project or study, and deadlines for completion. Within the parameters of the approved project plan, the incumbent is responsible for planning and organizing the study, and conducting all phases of the project. The incumbent informs the supervisor of potentially controversial findings, issues, or problems with widespread impact. Completed work is reviewed by the supervisor for effectiveness and compatibility with the current mission objectives and success in obtaining acceptance of recommendations by leadership.

Factor 3, Guidelines Level 3-4 450 Points

Guidelines include the Privacy Act of 1974 (as amended), Section 803 of Public Law 110-53 (Implementing Recommendations of the 9/11 Commission Act of 2007), E-Government Act, portions of the Federal Information Security Modernization Act (F1SMA), various OMB circulars and memoranda, National Institute of Standards and Technology Guidelines, and Office of the Federal Register policies. Guidelines consist of general administrative policies and management and organizational theories requiring considerable adaptation and/or interpretation for application to issues and problems studied. Policies and precedents provide a basic outline of the results desired, but do not go into detail as to the methods used to accomplish the project. Guidelines require considerable judgment and adaptation to tailor the guidelines to specific unique agency requirements. Within the context of broad regulatory guidelines, the employee must typically refine and develop more specific guidelines to complete the required planning and programming requirements.

Factor 4, Complexity Level 4-5 325 Points

The work consists of projects and studies which require analysis of interrelated issues of effectiveness, efficiency, and productivity of substantive specific [Agency] unique programs (i.e. Privacy). Typical assignments require developing and coordinating detailed plans, goals, and objectives for long-range implementation of the program. Decisions about how to proceed in planning, organizing, and conducting studies are complicated by conflicting program goals and objectives which may derive from changes in legislative or regulatory guidelines, productivity, and/or variations in the demand for program services. Assignments are further

complicated by the need to deal with subjective concepts such as value judgments; the quality and quantity of actions that are measurable primarily in predictive terms; and findings and conclusions are highly subjective and not readily susceptible to verification through replication of study methods or reevaluation of results. Options, recommendations, and conclusions developed by the employee take into account and give appropriate weight to uncertainties about the data and other variables that affect long range program performance. The employee must plan, coordinate, integrate, and implement the plans to support privacy requirements, integrating complex and widely varying privacy requirements. Develops innovative solutions and implements instructions for new policies and procedures.

Factor 5, Scope and Effect Level 5-4, 225 Points

The purpose of the work is to provide extensive knowledge and expertise in the direction, tracking, and integration of program review, analysis, and internal control efforts in the policy and operational area. The incumbent must possess and use a high degree of initiative, originality, foresight, and judgment to assure resolution of problems in a manner that solutions are accepted and implemented at the Department and Component levels.

Factor 6, Personal Contacts & Factor 7, Purpose of Contacts Level 6/7-C 180-Points

Personal contacts are with the [Agency] Component Privacy Officers, program managers, counsel, other agency officials and employees, and Federal and contract personnel of other agencies, e.g., Department of Justice. Incumbent participates, as a policy and technical expert, in meetings or conferences, as an authority on the [Agency] Privacy Program.

Contacts are for the purpose of review and coordination of the various work efforts to support the [Agency] Privacy Program to justify and resolve significant problems, and to provide expert policy and technical advice and consultation on a wide variety of issues and problems. Contact relationships also involve justifying, defending, negotiating, or settling significant program review and analysis issues as they arise, which require persuading others to modify initial positions on matters that may involve conflicting objectives and goals. The purpose and nature of the contacts require the incumbent to be the expert in all program review and analysis areas relating to the [Agency] Privacy Program.

Factor 8, Physical Demands Level 8-1 5 Points

Work is primarily sedentary, such as sitting comfortably. There may be some walking, standing, bending, carrying of light items.

No special physical effort or ability is required to perform the work.

Factor 9, Work Environment Level 9-1 5 Points

The employee works in an adequately lighted and ventilated office environment. Exercises normal safety precautions

Total Points = 3190 (3155 - 3600)

Grade = GS-13

2. 0343: Sample Job Announcement

Agency: [Insert name and logo]				
Job Announcement Number: [Insert number]				
Privacy Analyst (Privacy Program Specialist)				
SALARY RANGE: \$XX,XXX - \$XX,XXX USD per year	OPEN PERIOD: [Insert Opening to Closing Dates]			
SERIES & GRADE: GS-0343-9	POSITION INFORMATION: [Full-time/Permanent or Term as determined by agency]			
PROMOTION POTENTIAL: GS-0343-11 [As determined by agency]	LOCATIONS: [Insert Duty Location(s)]			
WHO MAY BE CONSIDERED: United States Citizens	If you identify your targeted applicant pool(s) in the Job Builder template, Career Patterns icons will be automatically inserted here, e.g., Time in Career, Mobility, etc.]			

Job Summary:

[Insert agency logo, optional]

[Insert information to attract your targeted talent pool(s) including agency's

branding/marketing/mission and work environment aspects e.g. telework, work schedules and other flexibilities. For help, go to <u>https://www.opm.gov/policy-data-oversight/human-capital-</u><u>management/#url=Framework</u>.]

Please see the sample language below.

Do you desire to protect American interests and secure our Nation while building a meaningful and rewarding career? If so, the [Agency] has the job for you.

In this role, the Privacy Analyst is responsible for supporting the Privacy Program, which includes understanding applicable legal, policy and technological requirements, communicating risks, and assessing and advising the agency in mitigating privacy risks in existing operations and new, planned data collections and technologies, ensuring compliance with applicable requirements and safeguarding the rights of the Federal Government and the public.

This position is located in the [Department], [Office]. The incumbent reports directly to the [Chief Privacy Officer] and advises the Director and the Deputy Assistant Secretary for [Office], as needed. The Privacy Analyst will advise, support, and assist the agency offices in their best efforts to establish information privacy and data protection initiatives, as well as in planning, implementing, and assessing their privacy programs.

Key Requirements:

- U.S. Citizenship or National
- Registered for Selective Service, if applicable (See <u>Other Information</u>)

- Meet specialized experience requirements (See <u>Qualifications and Evaluations</u>)
- Résumé and supporting documents (See How to Apply)
- Complete the <u>Occupational Questionnaire</u>
- Suitable for Federal employment

Great Benefits Package: paid vacation, sick days, holidays, health and life insurance, and an excellent retirement package!

Duties

The following are the duties of this position at the GS-11. If you are selected at a lower grade level, you will have the opportunity to learn to perform all these duties, and will receive training to help you grow in this position.

The incumbent of this position serves as a management analyst on the staff of the [Agency] Privacy Division with primary responsibility for evaluating the effectiveness of the [Agency] privacy program, researching new practices to improve efficiencies, overseeing [Agency] Component compliance with statutory and regulatory requirements related to the establishment and revision of Privacy Act systems of record notices (SORNs), the creation of Privacy Act procedural and exemption rules under the Administrative Procedures Act, the development and coordination of Privacy Act Computer Matching Agreements (CMAs), and the reporting and tracking of privacy incidents. In addition, the incumbent will support implementation of privacy program activities. The incumbent also supports oversight and management of other privacy compliance and risk management efforts.

The incumbent will:

- Analyze and evaluate the effectiveness of the privacy program in meeting its requirements and objectives, and advise management concerning effectiveness;
- Research and investigate new or improved business and management practices to strengthen the privacy program;
- Analyze new or proposed legislation or regulations to determine impact on program operations and management and ensure [Agency] Privacy Program compliance. Assess key business objectives, new product development concepts, proposed information collections and technology changes, and marketing initiatives being undertaken by [Agency offices] to develop and ensure implementation of privacy controls, and ensure appropriate authority to collect and data minimization.
- Ensure [Agency] use of appropriate privacy notices, e.g., SORNs, privacy impact assessments and privacy policies.
- Plan, develop, and deliver [Agency] wide privacy training materials for [Agency] Components. Training materials serve as a basis for providing training to agency personnel or as a template for the development of specialized training to be provided by the [Agency] Components.
- Provide training or briefings to [Agency] Component privacy officers and their staff for inperson/webinar/video-teleconference venues.
- Ensure accurate and timely information is posted to the [Agency] Privacy Office website and SharePoint site.
- The incumbent participates in special projects and initiatives and performs special assignments. Identifies the need for special projects and initiates milestones and goals.
- Evaluate reports by analyzing facts and performing appropriate research and prepares detailed responses.

- Determine appropriate recommendations for unresolved or questionable problems and performs follow-up.
- Research and determine or recommend appropriate actions or interpretation of issues impacting the serviced organizations.
- Represent [Agency] with a variety of organizations.
- Establish, develop, and maintain effective working relationships with customers; meet with key customer and coordinating officials to assess customer satisfaction, explain policy and procedures, and resolve problems.
- Provide or ensure subordinates provide customer guidance and training.
- Research and determine or recommend appropriate actions or interpretation of issues impacting the organization or agency.
- Prepare and present high-level briefings; prepare and analyze reports; respond to queries, justifications, and background papers on areas of expertise and assignment.
- Research and determine or recommend appropriate actions or interpretation of issues impacting the organization.
- At times, serve as the independent technical authority for the organization.
- Represent the organization on working groups; steering groups; or other meetings, conferences, seminars, etc. May chair such groups or meetings when the meeting is in the incumbents area of assignment.
- Promote interchange of information on Privacy requirements, capabilities, deficiencies, and technology applications.
- Defend recommendations to higher levels of management as necessary.

Qualifications and Evaluation

Qualifications Required:

You must meet the following requirements by the closing date of this announcement.

Specialized experience for the GS-09: You must have one year of specialized experience at a level of difficulty and responsibility equivalent to the GS-07 grade level in the Federal service. Specialized experience for this position is defined as experience in ALL of the following:

- Working in a team environment and providing customer service with an information management focus;
- Experience supporting compliance with the Privacy Act of 1974, and other related policies and guidance;
- Performing and completing a wide range of assignments related to privacy program activities, including review and drafting privacy policies, privacy impact assessments, explaining privacy related standards and requirements to other staff; analyzing privacy risks involving in proposed information collections; and
- Using project management methodologies to assist in planning and tracking projects.

OR

- master's or equivalent graduate degree
- OR
 - 2 full years of progressively higher level graduate education leading to such a degree

OR

LL.B. or J.D., if related.

The experience may have been gained in either the public, private sector or volunteer service. One year of experience refers to full-time work; part-time work is considered on a prorated basis. To ensure full credit for your work experience, please indicate dates of employment by month/day/year, and indicate number of hours worked per week on your resume.

[Agency must define specialized experience].

Your education, training, and/or experience must show that you possess the following competencies

- Privacy Technical Competencies
- Written Communication
- Oral Communication
- Interpersonal Skills
- Attention to Detail

How You Will Be Evaluated:

We will review your résumé to ensure you meet the basic qualification requirements. Applicants meeting basic qualification requirements will further be evaluated on the information provided in the Occupational <u>Questionnaire</u>. The <u>Occupational Questionnaire</u> collects information on your education, training, and experience related to critical competencies, such as project management, grants management, writing, oral communication, influencing/negotiating, problem solving, and attention to detail.

[Insert Agency Evaluation Procedure].

Benefits and Other Information

Benefits and Other Information:

Benefits:

Working for [Insert agency name] offers a comprehensive benefits package that includes, in part, paid vacation, sick leave, holidays, life insurance, health benefits, and participation in the Federal Employees Retirement System. [Insert agency specific benefits/flexibilities that may be attractive to potential applicants identified in your Career Patterns analysis, e.g., telework options, recruitment or relocation incentives, flexible work schedule, etc.] The following Web address is provided for your reference to explore the major benefits offered to most Federal employees. To find out more click here http://www.usajobs.opm.gov/ei61.asp.

Other Information:

Interagency Career Transition Assistance Program (ICTAP). The ICTAP provides eligible displaced Federal competitive service employees with selection priority over other candidates for competitive service vacancies. If your agency has notified you in writing that you are a displaced employee eligible for ICTAP consideration, you may receive selection priority if this vacancy is within your ICTAP eligibility, you apply under the instructions in this announcement, and you are found well-qualified for this vacancy. **[Insert agency definition of well-qualified.]** You must provide proof of eligibility with your application to receive selection priority. Such proof may include a copy of your written

notification of ICTAP eligibility or a copy of your separation personnel action form. Information about ICTAP eligibility is on OPM's Career Transition Resources website at <u>http://www.opm.gov/ctap/index.asp</u>.

[Insert the following paragraph if your agency did not clear CTAP before announcing outside its own workforce.]

Career Transition Assistance Plan (CTAP). The CTAP provides eligible surplus and displaced Federal competitive service employees with selection priority over other candidates for competitive service vacancies. If your agency has notified you in writing that you are a surplus or displaced employee eligible for CTAP consideration, you may receive selection priority if this vacancy is within your CTAP eligibility, you apply under the instructions in this announcement, and you are found well-qualified for this vacancy. [Insert agency definition of well-qualified.] You must provide a copy of your written notification of CTAP eligibility with your application. Information about CTAP eligibility is on OPM's Career Transition Resources website at http://www.opm.gov/ctap/index.asp.

Selective Service: If you are a male applicant born after December 31, 1959, you must certify that you have registered with the Selective Service System, or are exempt from having to do so under the Selective Service Law. See <u>www.sss.gov</u>.

Veterans' Preference: If you are entitled to veterans' preference, you should indicate the type of veterans' preference you are claiming on your résumé. Your veterans' preference entitlement will be verified by the employing agency.

- For 5-point veterans' preference, please provide your DD-214 (Certificate of Release or Discharge from Active Duty), official statement of service from your command if you are currently on active duty, or other official documentation (e.g., documentation of receipt of a campaign badge or expeditionary medal) that proves your military service was performed under honorable conditions.
- For 10-point veterans' preference, please submit a <u>Standard Form (SF) 15</u>, Application for 10-Point Veteran Preference and the required documentation.

How to Apply

How To Apply:

You may either 1) **APPLY ONLINE** or 2) deliver your application package via [Insert agency procedure.] Your complete application package will include:

- 3. Résumé
- 4. Occupational questionnaire
 - If you are applying online, <u>click here</u> to complete the Occupational Questionnaire
 - If you are NOT applying online,
 - i. <u>click here</u> to download the Occupational Questionnaire
 - ii. <u>click here</u> to download the form you must record your responses on

If faxing in your application package: Attention: [Insert name of contact] [Insert telephone number]				
Send Mail				
[Insert complete address] USA				
All electronic submissions or faxes must be submitted and received by [Insert time] Eastern Time [Insert closing date.] All mailed résumés and/or supporting documents must be received by [Insert closing date.] [Insert agency application receipt procedures if different.] What to Expect After You Apply:				
After all application packages have been received, we will review your résumé to ensure you meet the basic qualification requirements. We will evaluate each applicant who meets the basic qualifications on the information provided in the <u>Occupational Ouestionnaire</u> and may interview the best-qualified applicants. After making a tentative job offer, we will conduct a suitability and/or security background investigation. A final job offer for this position is typically made within 40 days after the deadline for applications.				
Questions?				
[Insert name of contact] Phone: [Insert contact's phone number including area code] TDD: [Insert TDD phone number including area code] Email: [Insert contact's email address]				
EEO Policy Statement				
EEO Policy Statement				
The United States Government does not discriminate in employment on the basis of race, color, religion, sex, national origin, political affiliation, sexual orientation, marital status, disability, age, membership in an employee organization, or other non-merit factor.				

Reasonable Accommodation Policy Statement

Federal agencies must provide reasonable accommodation to applicants with disabilities where appropriate. Applicants requiring reasonable accommodation for any part of the application and hiring process should contact the hiring agency directly. Determinations on requests for reasonable accommodation will be made on a case-by-case basis.

USAJOBS Control Number: [Insert number]

3. 0343: Sample Competencies and Interview Questions

0343 Sample Interview Questions

The interview questions below are categorized by high-level general or technical competencies, with some examples of more specific competencies that may be addressed. Some questions address more than one competency – some address many competencies – while others may only address one specific competency. These questions are intended to be a useful starting point for you to develop specific questions for a specific position. **Note**: The interviewer should explain to the applicant that, while the questions ask for examples and work experience, the applicant should not reveal any information that is sensitive or confidential to another organization.

Disclosure: A competency study will be completed to validate the competencies included in this toolkit and needed to perform privacy work government-wide. Also, please note that Federal regulations (5 C.F.R. Part 300.103) require that each employment practice be based on a job analysis. A job analysis must be completed to validate the competencies used to evaluate applicants for Federal positions.

Competencies 0343	Questions		
Analytical Reasoning	Q: How do you define privacy? What do you see as the biggest challenges to privacy protection today?		
Interpersonal Skills Includes Teamwork, Conflict Management, Influencing/Negotiating	Q: Please describe at least two situations where you worked on a team. What role did you have on the team, what went well, what were the challenges, and did the team accomplish its goals?		
Compliance Includes Authority to Collect, Purpose Specification, Accounting of Disclosures, Regulations and Policy, Accountability	Q: Please describe any processes or policies you have used or would recommend to ensure that your organization has authority to collect new data types.		
	Q: If a person sent an email to your organization that contained sensitive PII, but was not requested, does the organization have a privacy obligation to protect it, legal or otherwise? What actions should be taken?		
	Q: Please describe any experience you have had with procedures or processes to track disclosures (as required by the Privacy Act).		
	Q: What do you think about website privacy policies? Are they required? Needed? What should they cover? Why?		
Transparency Includes Transparency,	Q: What do you think about website privacy policies? Are they useful? What should they cover? Why?		
System of Records Notices and Privacy Act Statements	Q: What is a System of Records Notice (SORN), and why is a SORN important for the privacy program?		
	Q: What law mandates that a SORN be created, and how is the SORN communicated to the public?		

Competencies 0343	Questions	
	Q: What are the main challenges to effective mobile phone disclosures?	
Individual Participation and Redress Includes Individual Access,	Q: What do you view as the most effective ways to achieve consent to the handling and disclosure of PII? Do you see any challenges with how consent is handled with evolving technologies?	
Correction and Redress,	Q: Please describe any experience you have had responding to Privacy Act requests for access, correction or redress.	
	Q: If you were to receive a call or email from a member of the public with a privacy concern, what steps would you take to address the issue?	
Minimization	Q: How does your current employer define "sensitive PII"?	
Includes Minimization of PII, Minimization of PII Used in	Q: Does your current employer have a PII inventory? How was it created and how is it maintained?	
Testing, Training and Research, and Data Retention	Q: Please describe efforts you have taken in your work to minimize collection and retention of PII.	
and Disposal, Inventory of Personally Identifiable Information	Q: What questions or issues would you raise with a person who brings you a project that would involve collection and processing of sensitive PII?	
	Q: What is the value of an inventory of personally identifiable information? Please explain how you have helped develop or maintain such an inventory.	
Use Limitation Includes Internal Use	Q: Describe how you interpret the requirements to share information internally only with those who "need to know" the information, and the processes put in place to implement this requirement.	
	Q: What measures have you helped implement to ensure that PII is only shared externally as authorized?	
Policy Analysis and Development	Q: What are some of the most effective privacy or security policies you have read? What elements made them effective?	
	Q: Explain the difference between answering a question with "what is legally acceptable" vs. "what is the right thing to do?" Have you faced this question in your work?	
	Q: Describe privacy-related policies you have drafted or had input into, and any challenges you faced in drafting, organizational adoption of the policy, or implementation.	
Privacy Awareness and	Q: Describe situations where you have had to train other individuals.	
Training	Q: How are your organization's on-boarding and annual privacy training programs handled, and what are the key topics in those programs?	
	Q: In addition to annual training, what other types of privacy training does your organization provide and how are you involved?	
	Q: What has been your most effective staff awareness activity?	

Competencies 0343	Questions			
	Q: [mid to senior level position] Describe the types of privacy training you have delivered, the audience for that training, and any reactions or outcomes you recall from the training.			
	Q: [mid to senior level position] What format of training have you found to be most effective?			
Continual Learning (General Competency)	Q: How do you keep up with changes to privacy laws, policies and standards?			
	Q: What was the last training or privacy program you attended?			
Privacy Impact and Risk Assessment Includes Privacy Risk Management/ATOs, Security	Q: If an employee brought to you a project involving collection of new types of sensitive PII, where would you start in analyzing the project and providing guidance? What protections would you want in place and why?			
	Q: What do you think are the top three privacy risks in most Government Agencies?			
	Q: What is a Privacy Impact Assessment (PIA) and when should a PIA be performed?			
	Q: What are the benefits of a privacy specialist reviewing and approving a PIA, rather than leaving it up to the IT group or others?			
	Q: Please explain the types of risks you have identified in conducting PIAs and how you have mitigated those risks.			
	Q. Provide examples of the privacy controls described in NIST Spec. Pub. 800-53, Revision 4, and tell us your experience in developing, implementing and assessing the effectiveness of privacy controls.			
	Q: As part of a small team, how would you implement "privacy by design" (PbD)? How would you gain access to the system developers to influence them to adopt PbD standards in the system development lifecycle? What obstacles have you encountered in your organization in implementing PbD?			
Privacy Incident Response Includes Incident	Q. In your own words, what is a PII data breach and, as the privacy specialist, what would you want to know about such a breach?			
Management	Q: Have you ever been involved in helping respond to a breach of personal data or other data security incident? Describe your experience and role, if any, in investigating the breach or other incident, providing notice to affected individuals, determining what steps should be taken to mitigate the breach or incident, developing strategies for avoiding similar breaches or incidents in the future, other lessons learned.			
	Q: What is the importance of notification of affected individuals when data breaches occur?			

Competencies 0343	Questions	
Information Sharing With Third Parties Includes Privacy Requirements for Contractors and Service Providers,	 Q: Describe your experience with retaining and using contractors that handle or process PII, or if you have not had this experience, what issues would you expect to address? What actions have you taken, or would you take, to ensure that PII is sufficiently protected? Q: Describe ways that you could assure yourself that a service provider is actually doing what it cause it is doing. 	
<i>Contract and Grant Oversight</i> Privacy Reporting	is actually doing what it says it is doing. Q: Have you participated in providing written reports to your senior staff, Congress, OMB or other government agencies (or if private sector, your Board of Directors)? Q. What is FISMA and how does FISMA apply to your agency's privacy	
	program? Q: [mid to senior level] Please describe the types of briefings or presentations you have provided to your senior staff, Congress, or others (or if privacy sector, Board of Directors).	

<u>Appendix D: General Attorney (CPO, Privacy Counsel or Senior Privacy</u> <u>Counsel), GS-0905</u>

<u>1. 0905: Sample Position Description</u>

General Attorney, GS-905-12 Organizational Title: Privacy Counsel

Position Description

<u>INTRODUCTION</u>

[Brief description of agency's mission and privacy program.] This position is located in [agency office]. The incumbent reports directly to [SAOP or CPO]. Within applicable legal and policy requirements, the incumbent is responsible for participating in the promotion of openness and interoperability by providing support and legal advice for agency privacy program activities, which includes understanding applicable legal and policy requirements, communicating risks, and assessing and advising the agency in mitigating privacy risks in existing operations and new, planned data collections and technologies, ensuring compliance with applicable law and policy and safeguarding the legal and financial rights of the Federal Government and the public. The incumbent must have a law degree and be a member of a bar in good standing.

MAJOR DUTIES

Incumbent provides legal advice concerning proposed legislation, regulations or policy initiatives that may impact the [Agency], drafts regulations or policy initiatives to support the [Agency] mission and enhance data protection and privacy rights. Also provides legal advice/opinions, guidance, analytical and operational support for the [Agency] privacy program to ensure integration of privacy program requirements into all aspects of [Agency] operations, and compliance with law, regulations, guidelines and standards. The incumbent will be responsible for:

- Monitoring, analyzing and ensuring compliance with privacy laws and requirements, regulations and policies, including the US Constitution, Privacy Act of 1974, E-Government Act, privacy-related directives or other guidance (e.g., Office of Management and Budget, Dep't of Homeland Security, Nat'l Institute of Standards and Technology); effectively communicating legal advice and other requirements in writing and orally to other staff as appropriate;
- Analyzing current and planned policies and activities, and assessing [Agency] compliance with requirements; analyzing proposed privacy-related laws or requirements to determine if changes would impact organizational activities or privacy policies and advising [Agency] staff accordingly;
- Advising staff in mitigating privacy risks and ensuring compliance, and considering creative solutions to mitigating risks while achieving key mission objectives;
- Developing, updating and implementing privacy related policies, procedures, and guidance, including but not limited to: guidance on safeguarding personally identifiable information (PII); minimizing PII; retention and disposal of PII; authorized sharing of PII; accounting of disclosures; maintaining data quality and integrity; and receiving,

managing and responding to Privacy Act requests for access to information and correction, and redress;

- [Supervising all assigned cases from their inception and providing counsel for the preparation of cases for administrative review or court presentation to adequately protect the interests of the Government.]
- Representing Agency and Privacy Office staff in dealing with other components.
- [Participating with Agency trial attorney in any litigation which challenges the initial or appeal determination with respect to Privacy Act requests or denial of access to personal information under FOIA. Such assistance includes, but is not limited to, the preparation of "Vaughn" indexes to describe the documents or information withheld; the review, as requested, of all proposed filings to be made in the litigation, and the research into applicable case law or policy which would assist trial counsel.]
- Providing guidance on the legal and policy requirements pertaining to the release of information, Agency processing procedures, and precedential cases concerning dissemination of information.
- Reviewing legislation affecting privacy programs and activities; preparing comments on or recommending new or revised policies, regulations, and guidelines based on assessments of impact.
- Developing and implementing processes and procedures to assess privacy risks of proposed new data collections early in the agency's decision-making process; for each data collection, ensure [Agency] has legal authority to collect and that [Agency] will only use PII for the purposes stated in privacy notices and for compatible purposes; and that the agency only collects PII relevant and necessary for the purposes of collection;
- Reviewing, analyzing and/or developing proposed rulemakings under the Administrative Procedure Act, regulations, guidelines or other documents to determine privacy impacts, communicating those impacts to the appropriate [Agency] team, providing legal advice to team, and working with team to revise rulemaking or other documents to mitigate risks;
- Identifying privacy risks using risk assessment methods and tools, and analyzing privacy risks when new technologies or business processes, or material changes to technologies or business processes, are being considered, leveraging a privacy threshold analysis process;
- Participating on the [Agency] Change Control Board to ensure appropriate privacy review of any material changes to the [Agency] production network involving PII;
- Developing and ensuring implementation of privacy controls in the design of new or materially modified technologies or business processes; document such controls in privacy plans for specific systems and assess the effectiveness of such controls for the system review and approval process and regularly afterward; in coordination with [Office of Information Technology (OIT)], review each proposed "authority to operate," make recommendations to [Manager/CPO/SAOP] concerning privacy risks and approval, and document plans for strengthening privacy controls as appropriate;
- Developing, maintaining and regularly updating the [Agency's] inventory of its holdings of PII; work with staff to minimize holdings of PII, and in particular, social security numbers, in accordance with data retention and disposal requirements; work to minimize uses of PII in testing, training and research and ensure protection of PII that continues to be used in testing, training and research;
- Reviewing uses of PII, within the [Agency] and with third parties, and work with staff to ensure uses comply with the Privacy Act and privacy notices, and are compatible with the purposes for which the PII was collected; for information sharing outside the [Agency], assist in developing and implementing controls to protect PII and privacy rights through letters of intent, memorandum of understanding, contracts, agreements or international arrangements;

- Conducting due diligence of prospective contractors or grantees to ensure they can meet privacy requirements; ensuring that privacy requirements are included in contract, acquisition or grant-related documentation; and ensuring that audits/reviews of compliance with privacy requirements are conducted regularly during performance;
- Developing and implementing processes to track disclosures outside the [Agency] according to the Privacy Act;
- Developing and updating legally required privacy notices, including system of records notices (SORNs), privacy impact assessments (PIAs), agency privacy policies, and Privacy Act 5 U.S.C. 552a(e)(3) notices, ensure that the purpose for collection is specified in privacy notices, that individuals are provided an opportunity to consent to data collection when appropriate, that individuals are advised of how to access and correct information about them, and how to contact the [Agency] for complaints or redress;
- Developing and maintaining complaint management procedures to allow members of the public or agency staff to submit complaints and to ensure that the privacy program staff timely respond to such complaints and address issues; develop and maintain recordkeeping system for complaints and responses, and regularly review complaints and responses to determine performance metrics and adjust existing privacy practices to minimize complaints;
- Promoting privacy training and awareness efforts, drafting privacy training and awareness plans; developing and delivering privacy training, including training for new staff, annual training and role-based training, and awareness programs, including useful privacy information on the [Agency] intranet site, guest speakers, and newsletters, blogs or other special communications;
- Preparing reports to the Office of Management and Budget, Congress, other oversight body and organizations as needed, e.g., SAOP FISMA Report;
- Promptly preparing responses to questions from staff about handling PII, privacy risks and ways to improve business processes or otherwise mitigate risks, with compliance and also customer service in mind;
- Developing and implementing technologies, principles and processes to analyze, prioritize and respond to incidents involving loss or unauthorized access to PII; assist in responding to incidents, and maintaining documentation of incidents;
- Keeping abreast of changes to privacy laws and requirements, and as opportunities arise, participate in interagency privacy working groups to learn best practices;
- Coordinating privacy laws, requirements, policies and procedures, with records management, information technology, FOIA, e-discovery and other information governance functions;
- Ensuring compliance with the Paperwork Reduction Act in rulemakings and operations;
- Drafting and, as requested, delivering reports and briefings to senior executives, managers and other staff, as needed, on program operations or project status related to highly sensitive, complex and controversial privacy issues;
- Support agency response to incidents involving loss or unauthorized access to PII, maintain documentation of incidents, and regularly review incidents to understand patterns and develop mitigation measures;

Performs other related duties as assigned.

FACTOR 1 - KNOWLEDGE REQUIRED BY THE POSITION, FL 1-7 1250 Points

• The position requires the incumbent to be a licensed member of a state Bar in good standing.

- Comprehensive knowledge of, and demonstrated experience with independently applying Privacy Act, FISMA and e-Government requirements and guidelines to solve complex problems and legal issues related to Privacy.
- Comprehensive knowledge of the Agency statutory obligations, functions, and legal programs and operations.
- Skill in legal research and analytical and legal reasoning.
- Skill in preparing legal documents, correspondence, and affidavits.
- Skill in representing the agency on issues related to privacy.
- Ability to use various software (Microsoft Word, Excel, PowerPoint, Visio and Access) to extract data, create reports, monitor and evaluate program operations.
- Ability to apply analytical and evaluative methods to conduct reviews and studies of agency privacy programs, and make recommendations for privacy program improvements.
- Ability to communicate in writing sufficient to prepare privacy program documentation, briefs, reports, analyses, training materials, emails, web site information and required notices.
- Ability to collaborate and maintain effective working relationships with a wide range of individuals both internally and externally.
- Skill in planning and organizing several major projects simultaneously.
- High level of skill in communicating ideas and recommendations to senior Government officials in a manner that supports acceptance of positions.

FACTOR 2. SUPERVIOSRY CONTROLS, FL 2-4 450 Points

Incumbent works under the direction of the Chief Privacy Officer or his/her designee, who provides policy guidance, assignment areas, and special projects. The incumbent is guided by Federal laws, regulations, and Agency policy. Within this broad framework, the incumbent exercises initiative, and sound judgment in legal matters for Agency.

FACTOR 3. GUIDELINES, FL 3-4 450 Points

Guidelines include the Privacy Act of 1974, E-Government Act, Electronic Communications Privacy Act, Computer Fraud and Abuse Act, other civil and criminal laws, and opinions, civil service and Federal labor law, Federal regulations, and Agency orders. The incumbent must use initiative, mature judgment, and resourcefulness in researching and interpreting legal issues in the absence of clearly applicable precedents, evaluating complex facts and cases, determining difficult questions of law, and recommending a final agency decision. The incumbent also has responsibility for recommending and formulating policy changes when necessary.

FACTOR 4. COMPLEXITY, FL 4-5, 325 Points

The work involves serving as an Attorney-Advisor on matters pertaining to the role and functions of the Agency Privacy Office staff. Included are providing direct legal interpretations and legal advice and guidance to Agency managers, and their staff on a variety of issues, cases, and questions. The issues and matters for which the incumbent provides legal advice and counsel are complex due to the absence of clearly applicable precedents resulting in policy and operational concern.

Decisions regarding what needs to be done and how to proceed are complicated by the effects of legislative changes and conflicting program goals.

FACTOR 5. SCOPE AND EFFECT, FL 5-4, 225 Points

The purpose of the work is to provide legal support and advice to the Privacy Office staff with respect to policy development, program management and implementation, issue and problem analysis and resolution, representation and liaison in all phases of the functions and work of the office.

Legal advisory services regarding legal interpretation and legislative changes, affects the agencies' privacy program and its effectiveness and compliance.

FACTOR 6. PERSONAL CONTACTS, FL 6-3, and FACTOR 7. PURPOSE OF CONTACTS, FL 7-C 180 Points

The incumbent establishes and maintains continuing contacts and consultative relationships with senior agency management, officials and peers in the Agency, officials of other agencies, and members of the private bar.

Contacts are to represent the office; provide legal advice and consultation and confer on critical

and urgent issues, questions, problems, and matters; identify and discuss emerging issues and

positions; justify and defend decision; and provide guidance and assistance to the staff.

FACTOR 8. PHYSICAL DEMANDS, FL 8-1, 5 Points

The work is primarily sedentary where no special physical demands are necessary. Travel may be necessary.

FACTOR 9. WORK ENVIRONMENT, FL 9-1, 5 Points

The work is performed in an office setting.

Total Points: 2890 GS-12 Range 2755-3150

Evaluation Statement Summary

Title, Series, Grade: Attorney-Advisor, GS-905-12 Position Number: Classification Standard(s): OPM PCS GS-905, 05/74 Organization:

Factor 1- Nature of Cases or Legal Problems

Sub-Factor	Evaluation	Level
Nature of Legal Questions	Difficult questions. Absence of clearly applicable precedents.	II
Impact of Cases or Legal Problems	Problems assigned directly affect parties concerned and overall privacy program	II
Monetary Impact	Large sums of money are directly or indirectly involved	II
SUMMARY EVALUATION: II		
	Factor 2- Level of Responsibility	
Nature of Functions	Advises Chief Privacy Officer on a wide spectrum of legal issues.	С
Supervision received	Performs work independently to plan work.	С
Personal Contacts	Advises senior Agency staff, and component officials.	С
Nature and Scope of Recommendations & Decisions	Advices on complex legal questions/issues. Researches and interprets application of law. Prepares necessary briefings and opinions.	С

SUMMARY EVALUATION: C

Grade-Level Conversion: Type II Cases; Degree C Level of Responsibility Converts to GS-12.

2. 0905: Sample Job Announcement

Agency: [Insert name and logo]				
Job Announcement Number: [Insert number]				
Privacy Counsel, GS-0905-12				
SALARY RANGE: \$XX,XXX - \$XX,XXX USD per year	OPEN PERIOD: [Insert Opening to Closing Dates]			
SERIES & GRADE: GS-0905-12	POSITION INFORMATION: [Full-time/Permanent or Term as determined by agency]			
PROMOTION POTENTIAL: [As determined by agency] WHO MAY BE CONSIDERED: United States Citizens	LOCATIONS: [Insert Duty Location(s)] If you identify your targeted applicant pool(s) in the Job Builder template, Career Patterns icons will be automatically inserted here, e.g., Time in Career, Mobility, etc.]			

Job Summary:

[Insert agency logo, optional]

[Insert information to attract your targeted talent pool(s) including agency's

branding/marketing/mission and work environment aspects e.g. telework, work schedules and other flexibilities. For help, go to <u>https://www.opm.gov/policy-data-oversight/human-capital-</u><u>management/#url=Framework</u>.]

Please see the sample language below.

Do you desire to protect American interests and secure our Nation while building a meaningful and rewarding career? If so, the [Agency] has the job for you.

In this role, the Privacy Counsel is responsible for participating in the promotion of openness and interoperability which includes understanding applicable legal and policy requirements, communicating risks, and assessing and advising the agency in mitigating privacy risks in existing operations and new, planned data collections and technologies, ensuring compliance with applicable law and policy and safeguarding the legal and financial rights of the Federal Government and the public.

Great Benefits Package: paid vacation, sick days, holidays, health and life insurance, and an excellent retirement package!

Key Requirements:

- U.S. Citizenship or National
- Registered for Selective Service, if applicable (See <u>Other Information</u>)
- Meet specialized experience requirements (See <u>Qualifications and Evaluations</u>)
- Résumé and supporting documents (See How to Apply)
- Complete the <u>Occupational Ouestionnaire</u>
- Suitable for Federal employment

Duties

The Privacy Counsel provides legal advice concerning proposed legislation, regulations or policy initiatives that may impact the [Agency], drafts regulations or policy initiatives to support the [Agency] mission and enhance data protection and privacy rights. Also provides legal advice/opinions, guidance, analytical and operational support for the [Agency] privacy program to ensure integration of Privacy program requirements into all aspects of [Agency] operations, and compliance with law, regulations, guidelines and standards. In addition, the privacy counsel will be responsible for:

- Monitoring, analyzing and ensuring compliance with privacy laws and requirements, including the US Constitution, Privacy Act of 1974, E-Government Act, Electronic Communications Privacy Act, Computer Fraud and Abuse Act, other civil and criminal laws, and case law, as needed; effectively communicating legal advice and other requirements in writing and orally to other staff as appropriate;
- Analyzing current and planned policies and activities, and assessing [Agency] compliance with requirements; analyzing proposed privacy-related laws or requirements to determine if changes would impact organizational activities or privacy policies and advising [Agency] staff accordingly;
- Advising staff in mitigating privacy risks and ensuring compliance, and considering creative solutions to mitigating risks while achieving key mission objectives;
- Developing, updating and implementing privacy related policies, procedures, and guidance, including but not limited to: guidance on safeguarding personally identifiable information (PII); minimizing PII; retention and disposal of PII; authorized sharing of PII; accounting of disclosures; maintaining data quality and integrity; and receiving, managing and responding to Privacy Act requests for access to information and correction, and redress;
- Providing guidance on the legal and policy requirements pertaining to the release of information, Agency processing procedures, and precedential cases concerning dissemination of information.
- Reviewing legislation affecting Privacy programs and activities; preparing comments on or recommending new or revised policies, regulations, and guidelines based on assessments of impact.
- Developing and implementing processes and procedures to assess privacy risks of proposed new data collections early in the agency's decision-making process; for each data collection, ensure [Agency] has legal authority to collect and that [Agency] will only use PII for the purposes stated in privacy notices and for compatible purposes; and that the agency only collects PII relevant and necessary for the purposes of collection;
- Reviewing, analyzing and/or developing proposed rulemakings under the Administrative Procedure Act, regulations, guidelines or other documents to determine privacy impacts, communicating those impacts to the appropriate [Agency] team, providing legal advice to team, and working with team to revise rulemaking or other documents to mitigate risks;

- Identifying privacy risks using risk assessment methods and tools, and analyzing privacy risks when new technologies or business processes, or material changes to technologies or business processes, are being considered, leveraging a privacy threshold analysis process;
- Participating on the [Agency] Change Control Board to ensure appropriate privacy review of any material changes to the [Agency] production network involving PII;

Qualifications and Evaluation

Qualifications Required:

GS-12: You qualify at the GS-12 level if you possess one (1) year of specialized experience, equivalent to at least the GS-11 level in the Federal Government, which has equipped you with the skills needed to successfully perform the duties of the position. You must have experience performing the following duties:

Have at least 1 full year of specialized experience equivalent to the GS-11 level in the Federal service which provided you with the particular knowledge, skills, and abilities to perform the duties of the position. Qualifying specialized experience must demonstrate the following:

- Assisting in interpreting statutes, policies, and regulations to assess proper implementation in varying factual scenarios, assessing privacy risks, and communicating risks to other staff members,
- Providing legal advice to clients concerning data protection, privacy or other law, information management or public policy issues, and
- Applicants must be law school graduates with LL.B. or J.D. degrees AND applicants must be an active member in good standing of a state, territory of the United States, District of Columbia, or Commonwealth of Puerto Rico bar.

[Agency must define specialized experience].

Your education, training, and/or experience must show that you possess the following competencies

- Privacy Technical Competencies
- Legal, Government and Jurisprudence
- Written Communication
- Oral Communication
- Interpersonal Skills
- Attention to Detail

How You Will Be Evaluated:

We will review your résumé to ensure you meet the basic qualification requirements. Applicants meeting basic qualification requirements will further be evaluated on the information provided in the Occupational <u>Questionnaire</u>. The <u>Occupational Questionnaire</u> collects information on your education, training, and experience related to critical competencies, such as project management, writing, oral communication, influencing/negotiating, problem solving, and attention to detail.

Benefits and Other Information

Benefits and Other Information:

Benefits:

Working for [Insert agency name] offers a comprehensive benefits package that includes, in part, paid vacation, sick leave, holidays, life insurance, health benefits, and participation in the Federal Employees Retirement System. [Insert agency specific benefits/flexibilities that may be attractive to potential applicants identified in your Career Patterns analysis, e.g., telework options, recruitment or relocation incentives, flexible work schedule, etc.] The following Web address is provided for your reference to explore the major benefits offered to most Federal employees. To find out more click here http://www.usajobs.opm.gov/ei61.asp.

Other Information:

Interagency Career Transition Assistance Program (ICTAP). The ICTAP provides eligible displaced Federal competitive service employees with selection priority over other candidates for competitive service vacancies. If your agency has notified you in writing that you are a displaced employee eligible for ICTAP consideration, you may receive selection priority if this vacancy is within your ICTAP eligibility, you apply under the instructions in this announcement, and you are found well-qualified for this vacancy. **[Insert agency definition of well-qualified.]** You must provide proof of eligibility with your application to receive selection priority. Such proof may include a copy of your written notification of ICTAP eligibility or a copy of your separation personnel action form. Information about ICTAP eligibility is on OPM's Career Transition Resources website at http://www.opm.gov/ctap/index.asp.

[Insert the following paragraph if your agency did not clear CTAP before announcing outside its own workforce.]

Career Transition Assistance Plan (CTAP). The CTAP provides eligible surplus and displaced Federal competitive service employees with selection priority over other candidates for competitive service vacancies. If your agency has notified you in writing that you are a surplus or displaced employee eligible for CTAP consideration, you may receive selection priority if this vacancy is within your CTAP eligibility, you apply under the instructions in this announcement, and you are found well-qualified for this vacancy. **[Insert agency definition of well-qualified.]** You must provide a copy of your written notification of CTAP eligibility with your application. Information about CTAP eligibility is on OPM's Career Transition Resources website at http://www.opm.gov/ctap/index.asp.

Selective Service: If you are a male applicant born after December 31, 1959, you must certify that you have registered with the Selective Service System, or are exempt from having to do so under the Selective Service Law. See <u>www.sss.gov</u>.

Veterans' Preference: If you are entitled to veterans' preference, you should indicate the type of **veterans' preference you are** claiming on your résumé. **Your veterans' preference entitlement will be** verified by the employing agency.

- For 5-point veterans' preference, please provide your DD-214 (Certificate of Release or Discharge from Active Duty), official statement of service from your command if you are currently on active duty, or other official documentation (e.g., documentation of receipt of a campaign badge or expeditionary medal) that proves your military service was performed under honorable conditions.
- For 10-point veterans' preference, please submit a <u>Standard Form (SF) 15</u>, *Application for 10-Point Veteran Preference* and the required documentation.

Haw to Apply					
How to Apply					
How To Apply:					
You may either 1) (APPLY ONLINE) or 2) deliver your application package via [Insert agency procedure.] Your complete application package will include:					
 5. Résumé 6. Occupational questionnaire If you are applying online, <u>click here</u> to complete the Occupational Questionnaire If you are NOT applying online, i. <u>click here</u> to download the Occupational Questionnaire ii. <u>click here</u> to download the form you must record your responses on 					
If faxing in your application package: Attention: [Insert name of contact] [Insert telephone number]					
Send Mail					
[Insert complete address] USA					
All electronic submissions or faxes must be submitted and received by [Insert time] Eastern Time [Insert closing date.] All mailed résumés and/or supporting documents must be received by [Insert closing date.] [Insert agency application receipt procedures if different.]					
What to Expect After You Apply:					

After all application packages have been received, we will review your résumé to ensure you meet the basic qualification requirements. We will evaluate each applicant who meets the basic qualifications on the information provided in the <u>Occupational Questionnaire</u> and may interview the best-qualified applicants. After making a tentative job offer, we will conduct a suitability and/or security background

investigation. A final job offer for this position is typically made within 40 days after the deadline for applications.



[Insert name of contact] Phone: **[Insert contact's phone number including area code]** TDD: [Insert TDD phone number including area code] Email: [Insert co**ntact's email address]**

EEO Policy Statement

The United States Government does not discriminate in employment on the basis of race, color, religion, sex, national origin, political affiliation, sexual orientation, marital status, disability, age, membership in an employee organization, or other non-merit factor.

Reasonable Accommodation Policy Statement

Federal agencies must provide reasonable accommodation to applicants with disabilities where appropriate. Applicants requiring reasonable accommodation for any part of the application and hiring process should contact the hiring agency directly. Determinations on requests for reasonable accommodation will be made on a case-by-case basis.

DETAILED VERSION		
DETAILED VERSION	I CLOSE	PRINT

USAJOBS	Control	Number	Elnsert	numberl
USAJUBS	CONTROL	numper.	luser	number]



3. 0905: Sample Competencies and Interview Questions

0905 Sample Interview Questions

The interview questions below are categorized by some of the high-level general or technical competencies needed for positions in this job series, with some examples of more specific competencies that are also addressed. This list of competencies is not a complete, exhaustive list. Also, some questions address more than one competency – some address many competencies – while others may only address one specific competency. These questions are intended to be a useful starting point for you to develop specific questions for a specific position. **Note**: The interviewer should explain to the applicant that, while the questions ask for examples and work experience, the applicant should not reveal any information that is sensitive or confidential to another organization.

Disclosure: A competency study will be completed to validate the competencies included in this toolkit and needed to perform privacy work governmentwide. Also, please note that Federal regulations (5 C.F.R. Part 300.103) require that each employment practice be based on a job analysis. A job analysis must be completed to validate the competencies used to evaluate applicants for Federal positions.

Competencies - 0905	Questions
Analytical Reasoning	Q: How do you define privacy? What do you see as the biggest challenges to privacy protection today?
	Q: Why is privacy important for the government to maintain the public trust?
	Q: What do you see as the biggest challenges to privacy today?
Interpersonal Skills Includes Teamwork, Conflict Management, Influencing/Negotiating	Q: Please describe at least two situations where you worked on a team. What role did you have on the team, what went well, what were the challenges, and did the team accomplish its goals?
	Q: What experience have you had negotiating with or trying to influence other parties to agree with your position? What experience have you had mediating between two other parties? What lessons have you learned from your experiences?
Compliance Includes Policy Analysis & Development, Authority to Collect, Accounting of Disclosures	Q: Please describe any processes or policies you have used or would recommend to ensure that your organization has authority to collect new data types.
	Q: If a person sent an email to your organization that contained sensitive PII, but was not requested, does the organization have a privacy obligation to protect it, legal or otherwise? What actions should be taken?
	Q: Please describe any experience you have had with procedures or processes to track disclosures (as required by the Privacy Act).

Competencies - 0905	Questions
	Q: What do you think about website privacy policies? Are they required? Needed? What should they cover? Why?
	Q: How has your organization planned (is your organization planning) to implement revised OMB Circular A-130? What will be the most significant changes for how your program has been operating?
Transparency Includes Transparency,	Q: What do you think about website privacy policies? Are they useful? What should they cover? Why?
System of Records Notices and Privacy Act Statements	Q: What is a System of Records Notice (SORN), and why is a SORN important for the privacy program?
	Q: What law mandates that a SORN be created, and how is the SORN communicated to the public?
	Q: What are the main challenges to effective mobile phone disclosures?
Individual Participation and Redress Includes Consent, Individual Access, Correction and Redress, Complaint Management	Q: What do you view as the most effective ways to achieve consent to the handling and disclosure of PII? Do you see any challenges with how consent is handled with evolving technologies? What are some public considerations related to obtaining an individual's consent to use and/or disclose his or her PII?
	Q: How would you advise a program office that is planning to use an individual's PII for purposes other than originally stated in their public notices?
	Q: Please describe any experience you have had responding to Privacy Act requests for access, correction or redress.
	Q: If you were to receive a call or email from a member of the public with a privacy concern, what steps would you take to address the issue?
Privacy Law Includes Constitutional Law, Administrative Law, Criminal Law, Legal Analysis, and Legal, Government and	Q: Without disclosing confidential information, tell me about a time when you needed to research privacy laws, policies or other requirements. How did you go about the research; what were your findings; what went awry, or what would you do differently?
	Q: Who or what do you feel has done the most to strengthen privacy protections in the United States, historically or recently?
Jurisprudence	Q: Is there a right to privacy in the US Constitution?
	Q: What do you see as the potential legal concerns with emerging geo- location technology in items such as "smart" clothing, smart homes, and smart chips for pets?
	Q. Can an employee claim that his/her privacy has been violated if a fellow worker takes a picture of him/her on a smartphone in the workplace and posts it on Facebook?
	Q: Can a conversation or meeting at work be recorded without permission from those being recorded?
	Q: What is the e-Government Act, and what are agencies required to do pursuant to the Act?

Competencies - 0905	Questions
	Q: Do you see benefits with lawyers working in an organization's privacy program?
	Q: What is the Children's Online Privacy Protection Act (COPPA)? What are challenges today in complying with COPPA, given new technologies, big data analytics and marketing?
	Q: Explain your familiarity with the Administrative Procedure Act and the rulemaking process. Explain any experience in drafting rules for a government agency, or commenting on rules if in the private sector.
	Q: Have you addressed issues under the Electronic Communications Privacy Act (ECPA), or followed recent proposals for reform? Do you think ECPA needs to be amended, and if so, how?
	Q: What is your experience, if any, with the Privacy Act of 1974? Are you familiar with some of the interpretive problems with the Act, and if so, how would you fix them legislatively or otherwise?
	[Financial sector] Q: A database contains only information that is commonly found on the front of a personal check, including accountholder name, bank routing number, checking account number, payee and payment amount. Assuming that the operator of the database is a "financial institution" under the Gramm Leach Bliley Act (GLBA) and collected the information in connection with a financial service, is notice required before the institution collects this data? If there is an unauthorized access to the information, are consumer notifications required?
	<i>[Health sector]</i> Q: The Health Insurance Portability and Accountability Act (HIPAA) established important standards for the privacy and security of protected health information and the Health Information Technology for Economic and Clinical Health Act (HITECH) established breach notification requirements to provide greater transparency for individuals whose information may be at risk. Describe your experience working with HIPAA and HITECH Acts issues, and from a privacy legal perspective, what do you see as the challenges for enforcement and compliance.
	<i>[Health sector]</i> Q: The Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of HIPAA. What is the primary goal of the "Privacy Rule" and what are the challenges the goal presents?
	[Health sector] Q: What are some public considerations related to obtaining an individual's consent to use and/or disclose his or her PHI?
Minimization Includes Minimization of PII, Minimization of PII Used in Testing, Training and	Q: Do you work to develop or implement policies that define "sensitive PII"? If so, please explain the term "sensitive PII."

Competencies - 0905	Questions
Research, and Data Retention and Disposal,	Q: Does your organization have a PII inventory? If so, how was it created, and how is it maintained?
Inventory of Personally Identifiable Information	Q: Please describe efforts you have taken in your work to minimize collection and retention of PII.
	Q: What questions or issues would you raise with a person who brings you a project that would involve collection and processing of sensitive PII?
	Q: What is the value of an inventory of personally identifiable information? Please explain how you have helped develop or maintain such an inventory.
	Q: How would you interact with the person bringing you a project that had a lot of PII, what protections would you want in place and why?
	Q: What is anonymizing data and how does that differ from de- identifying data? How would you guide an organization in anonymizing or de-identifying data it plans to share with a third party?
Use Limitation Includes Internal Use	Q: Describe how you interpret the requirements to share information internally only with those who "need to know" the information, and the processes put in place to implement this requirement.
	Q: What measures have you helped implement to ensure that PII is only shared externally as authorized?
Data Quality and Integrity	Q: What are some ways an organization can help ensure data quality and integrity?
Policy Analysis and Development	Q: What are some of the most effective privacy or security policies you have read? What elements made them effective?
Includes Monitor and Analyze Privacy Law and Policies	Q: Explain the difference between answering a question with "what is legally acceptable" vs. "what is the right thing to do?" Have you faced this question in your work?
	Q: Describe privacy-related policies you have drafted or had input into, and any challenges you faced in drafting, organizational adoption of the policy, or implementation.
	Q: Have you followed proposed laws or amendments to laws that may impact your organization? Which laws and what types of impact did you recognize?
	Q: <i>[If agency collects and maintains data from the EU]</i> Please explain your familiarity if any with the EU General Data Protection Regulation (GDPR). If familiar with the GDPR, what do you see as the most significant impacts of the GDPR on U.S. organizations, either public or private sector?
	Q: <i>[If agency collects and maintains data from the EU]</i> What is your organization's legal basis for transferring personal data from the EU to the US, and how might that change under the GDPR? What do you see as

Competencies - 0905	Questions
	the most important aspect of the Court of Justice of the EU decision in the Maxx Schrems v. Commissioner of Ireland case?
Privacy Advice and Guidance	Q: Your responsibility includes supporting the organization's business operations by advising on privacy requirements. Explain scenarios where you have advised other employees on privacy requirements, your approach, what worked well, and what challenges you faced.
	Q: How do you measure the success of a privacy program/policy? What metrics might be important to collect and review?
	Q: Tell me about a time you influenced others to re-think a business approach because it raised significant privacy risks?
Privacy Awareness and	Q: Describe situations where you have had to train other individuals.
Training	Q: How are your organization's on-boarding and annual privacy training programs handled, and what are the key topics in those programs?
	Q: What has been your most effective staff awareness activity?
	Q: In addition to annual training, what other types of privacy training does your organization provide and how are you involved?
	Q: <i>[mid to senior level positions]</i> Describe the types of activities you have led on Data Privacy Day.
	Q: <i>[senior level position]</i> Describe the types of privacy training you have delivered, the audience for that training, and any reactions or outcomes you recall from the training.
	Q: <i>[mid to senior level position]</i> What format of training have you found to be most effective?
Continual Learning (General Competency)	Q: How do you keep up with changes to privacy laws, policies and standards?
	Q: What was the last training or continuing legal education (CLE) program you attended?
Privacy Impact and Risk Assessment Includes Privacy Risk Management/ATOs, Privacy Risk Management, Privacy by Design	Q: If an employee brought to you a project involving collection of new types of sensitive PII, where would you start in analyzing the project and providing guidance? What protections would you want in place and why?
	Q: What do you think are the top three privacy risks in most Government agencies?
	Q: What is a Privacy Impact Assessment (PIA) and when should a PIA be performed?
	Q: What are the benefits of a privacy specialist reviewing and approving a PIA, rather than leaving it up to the IT group or others?
	Q: Please explain the types of risks you have identified in conducting PIAs and how you have mitigated those risks.

Competencies - 0905	Questions
	 Q. Provide examples of the privacy controls described in NIST Spec. Pub. 800-53, Revision 4, and tell us your experience in developing, implementing and assessing the effectiveness of privacy controls.
	Q: What do you see as differences between information security and information privacy? And how are they aligned?
	Q: How have you, or would you, implement "privacy by design" (PbD)? How would you gain access to the system developers to influence them to adopt PbD standards in the system development lifecycle? What obstacles have you encountered in your organization in implementing PbD?
	Q: What are the most significant privacy risks with "big data"?
Privacy Incident Response Includes Incident Management	Q. In your own words, what is a PII data breach and, as the privacy specialist, what would you want to know about such a breach?
	Q: Have you ever been involved in helping respond to a breach of personal data or other data security incident? Describe your experience and role, if any, in investigating the breach or other incident, providing notice to affected individuals, determining what steps should be taken to mitigate the breach or incident, developing strategies for avoiding similar breaches or incidents in the future, other lessons learned.
	Q: What is the importance of notification of affected individuals when data breaches occur?
	Q: Explain any experience you have had in notifying appropriate Federal or state authorities about a data breach.
Information Sharing With Third Parties Includes Privacy Requirements for	Q: Describe your experience with retaining and using contractors that handle or process PII, or if you have not had this experience, what issues would you expect to address? What actions have you taken, or would you take, to ensure that PII is sufficiently protected?
Contractors and Service Providers, Contract and	Q: How would you assess third parties who handle PII on the organization's behalf?
Grant Oversight	Q: Describe ways that you could assure yourself that a service provider is actually doing what it says it is doing.
	Q: Are there privacy concerns with cloud storage technology? Does your organization use cloud technology, if so how are any privacy concerns addressed?
	Q: Explain any experience you have had in drafting agreements with third parties that contain privacy and security terms and conditions. What types of terms and conditions have you drafted or revised, or would you suggest be included in agreements?
Privacy Reporting	Q: Have you participated in providing written reports to your senior staff, Congress, OMB or other government agencies (or if private sector, your Board of Directors)?

Competencies - 0905	Questions
	 Q: [mid to senior level] Please describe the types of briefings or presentations you have provided to your senior staff, Congress, or others (or if privacy sector, Board of Directors). Q. What is FISMA and how does FISMA apply to your agency's privacy program? Have you prepared and delivered the SAOP report for FISMA? Q: Have you prepared and delivered reports under the Data Mining Reporting Act?
Privacy Monitoring and Auditing	 Q: How would you address gaps in privacy processes within an organization? Q: You have been tasked to conduct a privacy compliance review and present some recommendations to the organization about how PII data is handled. The organization is led by a senior executive who collects sensitive information from and about the public. You believe there is room for improvement in how public information is collected, managed, accounted for and secured. How would you approach this project in terms of tasks and major considerations?
Senior Level Positions: Governance and Privacy Program Includes Program Management, Developing Others, Leadership	 Q: What are some of the primary responsibilities of an organization's privacy program? Q: What do you view as the most effective organizational governance structure of a privacy program within an organization, e.g., reporting relationships? Q: Please describe your experience developing and implementing budgets. What key lessons have you learned from your experience? Q: Privacy leaders often dream of implementing the ideal privacy program, but the reality is often that the resources are not available. How would you manage a privacy program to make the most of the resources you have?
Supervisory Positions: Workforce Planning Includes Managing Human Resources, Developing Others, Employee Development	 Q: Explain your experience in workforce planning. Are you familiar with the parts of OMB revised Circular A-130 regarding workforce planning, and if so, how would you meet those requirements? Q: Please describe your experience managing other employees, including how you have developed employees. Q: What key lessons have you learned in your experience as a manager?

<u>Appendix E: IT Specialist (CPO, INFOSEC/Privacy Specialist, Privacy</u> <u>Program Manager, or Data Lifecycle Management and Privacy</u> <u>Protection), GS-2210</u>

<u>1. 2210: Sample Position Description</u>

IT Specialist (Privacy and Information Security Officer), GS-2210-12

Position Description

INTRODUCTION

The incumbent is responsible for providing support for agency privacy program activities, which includes understanding applicable requirements, communicating those risks, and assessing and supporting the agency in mitigating privacy risks in existing operations and new, planned data collections and technologies. The incumbent also will support the privacy program in drafting privacy-related reports to oversight bodies and for the Federal Information Security Modernization Act (FISMA), developing, implementing and maintaining privacy-related policies, procedures and controls, developing privacy notices to inform individuals about data handling and sharing practices, and training agency staff.

PRINCIPAL DUTIES AND RESPONSIBILITIES

The incumbent serves as a Privacy and Information Security Officer and participates with all echelons of management in planning, implementing, establishing and monitoring controls of the Automated Information Security (AIS) functions for a region with multiple subordinate facilities. Incumbent provides analytical and operational support for the privacy program to ensure integration of Privacy program requirements into all aspects of operations, and compliance with law, regulations, guidelines and standards.

The incumbent plans, develops, implements, and maintains programs, polices, and procedures to protect the integrity and confidentiality of systems, networks, and data. Designs, acquires, modifies, evaluates, and uses software intended to ensure that automated systems are secure from unauthorized use, viral infection, and other problems that would compromise classified information, confidentiality or privacy of data, or other aspects of overall Information Technology (IT) system security. Evaluates and implement new security authentication technologies. Recommends the acquisition of, implementation and dissemination of IT security tools, procedures, and practices to protect information assets. Develops privacy and IT security policy, guidelines, controls, and procedures for systems which are typically accessed by a large user community and which process multiple applications requiring differing privacy and security controls at multiple facilities. Plans and conducts security accreditation reviews for installed systems or networks, including reviewing privacy and security controls for the authority to operate, and recommends new or revised security measures and countermeasures based on results of reviews. Develops and/or interprets policy and procedural controls covering physical security, application and data security, system software security, contingency planning, and compliance. Updates

organization's contingency plans to respond to new privacy and security awareness training program for end users at all levels in the organization. Identifies and specifies information systems privacy and security requirements associated with migrations to new environments and provides guidance in planning and implementing migration activities. Develops specifications to ensure compliance with privacy and security requirements at the IT systems level. Coordinates the continuing AIS Privacy and Security Awareness and Training Program and works closely with area supervisors to facilitate the AIS Privacy and Security awareness effort. Prepares training material and conducts training sessions involving sensitive AIS for region management and system managers. Investigates privacy and security incidents and recommends appropriate action. Serves as a regional staff expert for dealing with violations for AIS privacy and security policy and systems. Maintains a historical file on AIS Privacy and Security related incidents. Performs other related duties as assigned.

The Privacy and Information Security Officer is responsible for all matters concerning information privacy and security procedures that assure compliance with the requirements of safeguarding personal and other sensitive data pursuant to the Computer Security Act of 1987, the Privacy Act of 1974, FISMA, E-Government Act, agency AIS Security Policy and Guidelines, and compliance with other laws and directives that protect the operational systems from waste, fraud or abuse.

- Develops, updates and implements privacy and security related policies, procedures, and guidance, including but not limited to: guidance on safeguarding personally identifiable information (PII); minimizing PII; retention and disposal of PII; authorized sharing of PII; accounting of disclosures; maintaining data quality and integrity; and receiving, managing and responding to Privacy Act requests for access to information and correction, and redress.
- Reviews existing regional information privacy and security policy for possible revision.
- Coordinates the continuing AIS privacy security awareness and training program by distributing applicable training information to the facility staff and works closely with the unit supervisors to facilitate the AIS privacy and security awareness effort.
- Prepares training material and conducts training sessions involving sensitive AIS privacy and security for regional management and system managers.
- Ensures procedures are established for proper disposition of forms and other printed output that contain sensitive data, and for controlling and authorizing movement of peripheral devices to off-site locations.
- Establishes and implements procedures for identifying and reporting suspected or actual AIS privacy and/or security breaches affecting physical environment and equipment, software, stored data, or computer outputs.
- Investigates privacy and security incidents and recommends appropriate action.
- Serves as a staff expert for dealing with violations for AIS privacy and security policy and systems. Maintains a historical file on AIS privacy and security related incidents.
- Independently initiates privacy and security reviews of services and operations.
- Reviews all technical privacy and security procedures and modifies as appropriate.
- Assures that procedures are developed and implemented to protect data transmission and storage media from unauthorized access.
- Reviews security software currently on the market, as appropriate coordinate's findings with appropriate staff, and recommends its use where appropriate.
- Assures software security is maintained, including the use and selection of software protection devices that prevent unauthorized access to system programs or data.
- Provides advice and guidance to ensure procedures are established for identifying and reporting incidents of physical security.

- Establishes, coordinates, and monitors policies and procedures to ensure physical security of computer systems and terminal devices, and access controls to software and data.
- Monitors systems and operating environment to ensure appropriate and timely action to protect assets from damage, destruction, alteration, and misappropriation.
- Ensures that privacy and security risk assessments are conducted on all systems and assuring the implementation of approved recommendations.
- Reviews and evaluates the impact of proposed facility changes in AIS security.
- Ensures that appropriate privacy and security risk management policies, procedures and controls are established and implemented throughout the information lifecycle, starting in the design phase of new data collections or systems; embed privacy and security controls into new data collections or systems; review/audit policies, procedures and controls regularly to ensure effectiveness and update as needed.
- Assist in developing and implementing privacy enhancing technologies, i.e., technologies that automate privacy controls on the collection, use, retention, and disclosure of PII;
- Ensures that procedures are developed for disaster prevention, emergency preparedness, contingency planning, and for back/up restart/recovery of computer systems.
- Coordinates the development of a contingency plan and updates annually or more frequently as required.
- Reviews and evaluates the results of contingency plan tests and reports findings with recommendations to superiors.
- Ensures the development of sensitive system privacy and security plans for each AIS that processes sensitive data.
- Reviews the effectiveness of the locally established AIS procedures as implemented.
- Maintains all AIS documentation files. Assures all AIS security reference material is current and up-to date.
- Assists in developing, maintaining and regularly updating the inventory of its holdings of PII; work with staff to minimize holdings of PII, and in particular, social security numbers, in accordance with data retention and disposal requirements; work to minimize uses of PII in testing, training and research and ensure protection of PII that continues to be used in testing, training and research;
- Regularly assists in reviewing uses of PII, within the organization and with third parties, and work with staff to ensure uses comply with the Privacy Act and privacy notices, and are compatible with the purposes for which the PII was collected; for information sharing outside the organization, assist in developing and implementing controls to protect PII and privacy rights through letters of intent, memorandum of understanding, contracts, agreements or international arrangements.
- Assists in conducting due diligence of prospective contractors or grantees to ensure they can meet privacy requirements and ensuring that audits/reviews of compliance with privacy requirements are conducted regularly during performance.
- Develops and updates legally required privacy notices, including system of records notices (SORNs), privacy impact assessments (PIAs), agency privacy policies, and Privacy Act 5 U.S.C. 552a(e)(3) notices, ensure that the purpose for collection is specified, that individuals are provided an opportunity to consent to data collection when appropriate, that individuals are advised of how to access and correct information about them, and how to contact for complaints or redress.
- Responsible for analytical functions relative to administrative and program aspects.

FACTOR 1 - Knowledge Required by the Position, FL 1-7 1250 Points

Knowledge of, and skill in applying IT security principles and methods; commercial systems security products; technical documentation methods; and performance management methods sufficient to carry out activities leading to security certification or accreditation, including addressing privacy related controls; conduct integrated analysis of multiple audit logs (e.g., firewall, Web server, etc.); identify violations and recommend corrective actions; and provide input in drafting information systems privacy and security documentation (e.g., systems security plans, privacy plans, privacy continuous monitoring strategies, risk assessments, disaster recovery plans, business continuity plans, and user security guides).

Knowledge of requirements analysis principles and methods, communications techniques, IT forensics principles, network operations and protocols, systems privacy and security regulations and policies sufficient to provide privacy and security advice and to develop privacy and security implementation plans which ensure proper protection of IT systems. Knowledge and skill in analysis and review techniques to evaluate and review AIS security programs.

Knowledge of configuration and data management to assist in ensuring the security of communications services and data, using encryption when appropriate, and using defensive measures to detect, respond and protect information, information systems and networks from threats.

Knowledge of the principles of administration, resource utilization, program planning, evaluation and management of staff and projects.

Knowledge and skill to anticipate and resolve AIS privacy and information security problems resulting from changing legal, policy and procedural requirements.

Knowledge of a wide range of IT design/diagnostic tools, principles, standards, precedents, techniques, requirements, methods, applications, sources, and procedures to perform a variety of assignments in the assigned application or specialty area.

Ability to communicate, orally and in writing, detailed technical information in a clear, logical and concise manner.

FACTOR 2 - Supervisory Controls, FL 2-4 450 Points

The supervisor outlines overall objectives and available resources. The employee and supervisor, in consultation, discuss timeframes, scope of the assignment including possible stages, and possible approaches.

The employee determines the most appropriate principles, practices, and methods to apply in all phases of assignments, including the approach to be taken, degree of intensity, and depth of research in management advisories; frequently interprets regulations on his/her own initiative, applies new methods to resolve complex and/or intricate, controversial, or unprecedented issues and problems, and resolves most of the conflicts that arise; and keeps the supervisor informed of progress and of potentially controversial matters.

The supervisor reviews completed work for soundness of overall approach, effectiveness in meeting requirements or producing expected results, the feasibility of recommendations, and adherence to requirements. The supervisor does not usually review methods used.
FACTOR 3 - Guidelines, FL 3-4 450 Points

Guidelines are multifaceted concerning automated information security and consist of broad systems and program directives; texts; laws; agency, Office of Management and Budget, and Government-wide regulations; local policies and memoranda; and general knowledge of agency practices. The employee uses a wide variety of reference materials and manuals; however, they are not directly applicable to issues and problems due to novel situations encountered. The employee uses judgment, initiative, and resourcefulness in deviating from established methods to modify, adapt, and/or refine broader guidelines to resolve specific complex and/or intricate issues and problems; treat specific issues or problems; research trends and patterns; develop new methods and criteria; and/or propose new policies and practices.

FACTOR 4 – Complexity, FL 4-4 225 Points

Duties consist of a wide variety of activities, such as planning, implementing and evaluating effectiveness of AIS Information Security programs; assessing the security effectiveness of installed systems based on analysis of reported privacy and/or security problems; implementing modifications to minimize vulnerabilities; troubleshooting privacy and security threats and vulnerabilities in response to incident reports;

Identifying and isolating problem sources; determining the need for new or updated privacy or IT security guidance based on policy and technology changes and recommending solutions and/or correcting problems to avert potential systems, data, or network exposure. The employee exercises judgment to continually evaluate and recommend the adoption of new privacy and IT security methods that will enhance capabilities.

FACTOR 5 - Scope and Effect

The purpose of this position is to establish and implement AIS security program within the region and to provide assistance to management in the area of AIS privacy and security. Work involves developing, implementing, and administering a privacy and IT security program consisting of standards, procedures, and guidance designed to protect information available on a major wide area network. The work involves investigating and analyzing a variety of conditions; resolving problems; and/or developing, testing, and implementing new technologies.

Scope of work involves all users of AIS equipment in the region (including remote access). Includes security of all hardware, software, data access, usage, storage, and transmission.

Work contributes to ensuring confidentiality, integrity, and availability of systems, networks, and data.

FACTOR 6 - Personal Contact, FL 6-3 Points 180

Personal contacts will include staff within the facility and agency at all levels. Contacts, in addition to those within the agency, are with vendor representatives, consultants, computer personnel of other agencies, representatives of professional associations, or public interest groups, in moderately unstructured settings. Contacts may also include officials several managerial levels above the employee on an ad hoc or other irregular basis.

FACTOR 7 - Purpose of Contacts, FL 7-C Points combined with Factor 6

The purpose of contacts is to provide or receive information; provide administrative direction; exchange information; establish and implement an AIS privacy and security program including procedures for implementation, maintenance, and reporting; monitor AIS equipment usage; and to gain compliance with established policies and regulations.

In addition, contacts will be for the purpose of presenting observations and findings to administrative and operating officials; advising management of the benefits and disadvantages of recommendations, approaches, and solutions; and negotiating with administrative and operating officials to obtain agreement and/or understanding of recommendations and proposals.

Contacts with vendors, academia, and private sector individuals will be made to obtain knowledge regarding various software and AIS equipment.

FACTOR 8 - Physical Demands, FL 8-1, 5 Points

Work is mostly sedentary and does not require any special physical effort. Duties may require lifting and carrying computer equipment such as monitors and printers.

FACTOR 9 - Work Environment, FL 9-1, 5 Points

The work is performed in an office environment and at computer facilities. The work area is adequately lighted, heated and ventilated. The work environment involves everyday risks or discomforts that require normal safety precautions.

Total Points: 2790 GS-12 Range 2755-3150

2. 2210: Sample Job Announcement

Agency: [Insert name and logo]

Job Announcement Number: [Insert number]

IT Specialist (INFOSEC/Privacy Specialist), GS-2210-12

SALARY RANGE: \$XX,XXX - \$XX,XXX USD per year	OPEN PERIOD: [Insert Opening to Closing Dates]
SERIES & GRADE: GS-2210-12	POSITION INFORMATION: [Full-time/Permanent or Term as determined by agency]
PROMOTION POTENTIAL: [As determined by agency]	LOCATIONS: [Insert Duty Location(s)]
WHO MAY BE CONSIDERED: United States Citizens	[If you identify your targeted applicant pool(s) in the Job Builder template, Career Patterns icons will be automatically inserted here, e.g., Time in Career, Mobility, etc.]

Job Summary: [Insert agency logo, optional]

[Insert information to attract your targeted talent pool(s) including agency's

branding/marketing/mission and work environment aspects e.g. telework, work schedules and other flexibilities. For help, go to <u>https://www.opm.gov/policy-data-oversight/human-</u> capital-management/#url=Framework.]

Please see the sample language below.

Do you desire to protect American interests and secure our Nation while building a meaningful and rewarding career? If so, the [Agency] has the job for you.

In this role you will support the [Agency] privacy program activities, which includes understanding applicable requirements, communicating those risks, and assessing and supporting the agency in mitigating privacy risks in existing operations and new, planned data collections and technologies. This position will support the privacy program in drafting privacy-related reports to oversight bodies and for the Federal Information Security Modernization Act (FISMA), developing, implementing and maintaining privacy-related policies and procedures, developing privacy notices to inform individuals about data handling and sharing practices, and training agency staff.

Great Benefits Package: paid vacation, sick days, holidays, health and life insurance, and an excellent retirement package!

Key Requirements:

- U.S. Citizenship or National
- Registered for Selective Service, if applicable (See <u>Other Information</u>)
- Meet specialized experience requirements (See <u>Qualifications and Evaluations</u>)
- Résumé and supporting documents (See How to Apply)
- Complete the Occupational Questionnaire
- Suitable for Federal employment

Duties

The Privacy and Information Security Officer is responsible for all matters concerning information security and privacy procedures that assure compliance with the requirements of safeguarding personal and other sensitive data pursuant to the Computer Security Act of 1987, the Privacy Act of 1974, E-Government Act, Federal Information Security Modernization Act (FISMA), agency AIS Security Policy and Guidelines, and compliance with other laws and directives that protect agency information and systems from loss or unauthorized access or disclosures.

The incumbent:

- Develops, updates and implements privacy and security related policies, procedures, and guidance, including but not limited to: guidance on safeguarding personally identifiable information (PII); minimizing PII; retention and disposal of PII; authorized sharing of PII; accounting of disclosures; maintaining data quality and integrity; and receiving, managing and responding to Privacy Act requests for access to information and correction, and redress;
- Coordinates the continuing privacy and security awareness and training program by distributing applicable privacy and security training information to the facility staff and works closely with the unit supervisors to facilitate the awareness efforts;
- Establishes and implements procedures for identifying and reporting suspected or actual privacy or security breaches affecting physical environment and equipment, software, stored data, or computer outputs.
- Serves as a staff expert for dealing with violations for privacy and security policy and systems. Maintains a historical file on privacy and security related incidents.
- Reviews all technical security procedures and modifies as appropriate.
- Assures that procedures are developed and implemented to protect data transmission and storage media from unauthorized access.
- Reviews privacy and security software currently on the market, as appropriate coordinate's findings
 with appropriate staff, and recommends its use where appropriate, with a particular focus on privacy
 enhancing technologies.
- Assures software security is maintained, including the use and selection of software protection devices that prevent unauthorized access to system programs or data.
- Provides advice and guidance to ensure procedures are established for identifying and reporting incidents of physical security.
- Establishes, coordinates, and monitors policies and procedures to ensure physical security of computer systems and terminal devices, and access controls to software and information.
- Monitors systems and operating environment to ensure appropriate and timely action to protect assets from damage, destruction, alteration, and misappropriation.

- Ensures that Risk Assessments are conducted on all systems and assuring the implementation of approved recommendations.
- Reviews and evaluates the impact of proposed facility changes in security.
- Ensures that appropriate privacy and security risk management procedures are established and implemented.
- Ensures that procedures are developed for disaster prevention, emergency preparedness, contingency planning, and for back/up restart/recovery of computer systems.
- Coordinates the development of a contingency plan and updates annually or more frequently as required.
- Reviews and evaluates the results of contingency plan tests and reports findings with recommendations to superiors.
- Ensures the development of sensitive system privacy and security plans for each business unit that processes sensitive information, including personally identifiable information (PII).
- Reviews the effectiveness of the locally established privacy and security procedures as implemented.
- Maintains all [privacy and security division] documentation files, and assures all privacy and security reference material is current and up-to date.
- Assists in developing, maintaining and regularly updating the inventory of its holdings of PII; work with staff to minimize holdings of PII, and in particular, social security numbers, in accordance with data retention and disposal requirements; work to minimize uses of PII in testing, training and research and ensure protection of PII that continues to be used in testing, training and research.
- Regularly assists in reviewing uses of PII, within the organization and with third parties, and work with staff to ensure uses comply with the Privacy Act and privacy notices, and are compatible with the purposes for which the PII was collected; for information sharing outside the organization, assist in developing and implementing controls to protect PII and privacy rights through letters of intent, memorandum of understanding, contracts, agreements or international arrangements.
- Assists in conducting due diligence of prospective contractors or grantees to ensure they can meet privacy requirements and ensuring that audits/reviews of compliance with privacy requirements are conducted regularly during performance.
- Develops and updates legally required privacy notices, including system of records notices (SORNs), privacy impact assessments (PIAs), agency privacy policies, and Privacy Act 5 U.S.C. 552a(e)(3) notices, ensure that the purpose for collection is specified, that individuals are provided an opportunity to consent to data collection when appropriate, that individuals are advised of how to access and correct information about them, and how to contact for complaints or redress.
- Responsible for analytical functions relative to administrative and program aspects.

Qualifications and Evaluation Qualifications Required:

GS-12: You qualify at the GS-12 level if you possess one (1) year of specialized experience, equivalent to at least the GS-11 level in the Federal Government, which has equipped you with the skills needed to successfully perform the duties of the position. You must have experience performing the following duties:

Have at least 1 full year of specialized experience equivalent to the GS-11 level in the Federal service which provided you with the particular knowledge, skills and abilities to perform the duties of the position. Qualifying specialized experience must demonstrate the following: applying privacy and security theories and concepts, practices, and emerging issues; and supporting working groups and others involved in privacy and cyber security in order to plan and coordinate organizational-wide implementation of privacy and security defense strategies to ensure protection of the **[agency's]**

information and infrastructure.

[Agency must define specialized experience].

Your education, training, and/or experience must show that you possess the following competencies

- IT Specialist Technical Competencies (e.g. Information Security)
- Program Management
- Written Communication
- Oral Communication
- Interpersonal Skills
- Customer Service
- Attention to Detail

How You Will Be Evaluated:

We will review your résumé to ensure you meet the basic qualification requirements. Applicants meeting basic qualification requirements will further be evaluated on the information provided in the Occupational <u>Questionnaire</u>. The <u>Occupational Questionnaire</u> collects information on your education, training, and experience related to critical competencies, such as project management, grants management, writing, oral communication, influencing/negotiating, problem solving, and attention to detail.

[Insert Agency Evaluation Procedure].

Benefits and Other Information Benefits and Other Information:

Benefits:

Working for [Insert agency name] offers a comprehensive benefits package that includes, in part, paid vacation, sick leave, holidays, life insurance, health benefits, and participation in the Federal Employees Retirement System. [Insert agency specific benefits/flexibilities that may be attractive to potential applicants identified in your Career Patterns analysis, e.g., telework options, recruitment or relocation incentives, flexible work schedule, etc.] The following Web address is provided for your reference to explore the major benefits offered to most Federal employees. To find out more click here http://www.usajobs.opm.gov/ei61.asp.

Other Information:

Interagency Career Transition Assistance Program (ICTAP). The ICTAP provides eligible displaced Federal competitive service employees with selection priority over other candidates for competitive service vacancies. If your agency has notified you in writing that you are a displaced employee eligible for ICTAP consideration, you may receive selection priority if this vacancy is within your ICTAP eligibility, you apply under the instructions in this announcement, and you are found well-qualified for this vacancy. **[Insert agency definition of well-qualified.]** You must provide proof of eligibility with your application to receive selection priority. Such proof may include a copy of your written

notification of ICTAP eligibility or a copy of your separation personnel action form. Information about ICTAP eligibility is on OPM's Career Transition Resources website at <u>http://www.opm.gov/ctap/index.asp</u>.

[Insert the following paragraph if your agency did not clear CTAP before announcing outside its own workforce.]

Career Transition Assistance Plan (CTAP). The CTAP provides eligible surplus and displaced Federal competitive service employees with selection priority over other candidates for competitive service vacancies. If your agency has notified you in writing that you are a surplus or displaced employee eligible for CTAP consideration, you may receive selection priority if this vacancy is within your CTAP eligibility, you apply under the instructions in this announcement, and you are found well-qualified for this vacancy. [Insert agency definition of well-qualified.] You must provide a copy of your written notification of CTAP eligibility with your application. Information about CTAP eligibility is on OPM's Career Transition Resources website at http://www.opm.gov/ctap/index.asp.

Selective Service: If you are a male applicant born after December 31, 1959, you must certify that you have registered with the Selective Service System, or are exempt from having to do so under the Selective Service Law. See <u>www.sss.gov</u>.

Veterans' Preference: If you are entitled to veterans' preference, you should indicate the type of veterans' preference you are claiming on your résumé. Your veterans' preference entitlement will be verified by the employing agency.

- For 5-point veterans' preference, please provide your DD-214 (Certificate of Release or Discharge from Active Duty), official statement of service from your command if you are currently on active duty, or other official documentation (e.g., documentation of receipt of a campaign badge or expeditionary medal) that proves your military service was performed under honorable conditions.
- For 10-point veterans' preference, please submit a <u>Standard Form (SF) 15</u>, *Application for 10-Point Veteran Preference* and the required documentation.

How to Apply

How To Apply:

You may either 1) **APPLY ONLINE** or 2) deliver your application package via [Insert agency procedure.] Your complete application package will include:

- 7. Résumé
- 8. Occupational questionnaire
 - If you are applying online, <u>click here</u> to complete the Occupational Questionnaire
 - If you are NOT applying online,
 - i. <u>click here</u> to download the Occupational Questionnaire
 - ii. <u>click here</u> to download the form you must record your responses on

If faxing in your application package: Attention: [Insert name of contact] [Insert telephone number]

Send Mail

[Insert complete address] USA

All electronic submissions or faxes must be submitted and received by [Insert time] Eastern Time [Insert closing date.] All mailed résumés and/or supporting documents must be received by [Insert closing date.] [Insert agency application receipt procedures if different.]

What to Expect After You Apply:

After all application packages have been received, we will review your résumé to ensure you meet the basic qualification requirements. We will evaluate each applicant who meets the basic qualifications on the information provided in the <u>Occupational Ouestionnaire</u> and may interview the best-qualified applicants. After making a tentative job offer, we will conduct a suitability and/or security background investigation. A final job offer for this position is typically made within 40 days after the deadline for applications.

? Questions?

[Insert name of contact] Phone: **[Insert contact's phone number including area code]** TDD: [Insert TDD phone number including area code] Email: **[Insert contact's email address]**

EEO Policy Statement

The United States Government does not discriminate in employment on the basis of race, color, religion, sex, national origin, political affiliation, sexual orientation, marital status, disability, age, membership in an employee organization, or other non-merit factor.

Reasonable Accommodation Policy Statement

Federal agencies must provide reasonable accommodation to applicants with disabilities where appropriate. Applicants requiring reasonable accommodation for any part of the application and hiring process should contact the hiring agency directly. Determinations on requests for reasonable accommodation will be made on a case-by-case basis.

DETAILED VE	RSION	X	CLOSE		PRINT
DETAILED VE	RSION	IX	CLOSE	-	PRINT

USAJOBS Control Number: [Insert number]



3. 2210: Sample Competencies and Interview Questions

2210 Sample Interview Questions

The interview questions below are categorized by some of the high-level general or technical competencies needed for positions in this job series, with some examples of more specific competencies that are also addressed. This list of competencies is not a complete, exhaustive list. Also, some questions address more than one competency – some address many competencies—while others may only address one specific competency. These questions are intended to be a useful starting point for you to develop specific questions for a specific position. **Note**: The interviewer should explain to the applicant that, while the questions ask for examples and work experience, the applicant should not reveal any information that is sensitive or confidential to another organization.

Disclosure: A competency study will be completed to validate the competencies included in this toolkit and needed to perform privacy work governmentwide. Also, please note that Federal regulations (5 C.F.R. Part 300.103) require that each employment practice be based on a job analysis. A job analysis must be completed to validate the competencies used to evaluate applicants for Federal positions.

Competencies-2210	Questions
Analytical Reasoning	Q: How do you define privacy? What do you see as the biggest challenges to privacy protection today?
	Q: Why is privacy important for the government to maintain the public trust?
Interpersonal Skills Includes Teamwork, Conflict Management, Influencing/Negotiating	Q: Please describe at least two situations where you worked on a team. What role did you have on the team, what went well, what were the challenges, and did the team accomplish its goals?
Compliance Includes Authority to Collect, Purpose Specification, Accounting	Q: Please describe any processes or policies you have used or would recommend to ensure that your organization has authority to collect new data types.
of Disclosures, Regulations and Policy, Accountability	Q: If a person sent an email to your organization that contained sensitive PII, but was not requested, does the organization have a privacy obligation to protect it, legal or otherwise? What actions should be taken?
	Q: Please describe any experience you have had with procedures or processes to track disclosures (as required by the Privacy Act).
	Q: What do you think about website privacy policies? Are they required? Needed? What should they cover? Why?
	Q: How has your organization planned (is your organization planning) to implement revised OMB Circular A-130? What will be the most significant changes for how your program has been operating?
Transparency	Q: What do you think about website privacy policies? Are they useful? What should they cover? Why?
Includes Transparency, System of Records Notices and Privacy Act Statements	Q: What is a System of Records Notice (SORN), and why is a SORN important for the privacy program?
	Q: What law mandates that a SORN be created, and how is the SORN communicated to the public?
	Q: What are the main challenges to effective mobile phone disclosures?

Individual Participation and Redress Includes Consent, Individual Access, Correction and Redress, Complaint Management	Q: What do you view as the most effective ways to achieve consent to the handling and disclosure of PII? Do you see any challenges with how consent is handled with evolving technologies? What are some public considerations related to obtaining an individual's consent to use and/or disclose his or her PII?
	Q: How would you advise a program office that is planning to use an individual's PII for purposes other than originally stated in their public notices?
	Q: Please describe any experience you have had responding to Privacy Act requests for access, correction or redress.
	Q: If you were to receive a call or email from a member of the public with a privacy concern, what steps would you take to address the issue?
Privacy-Enhancing System Design and Development	Q: What do you see as the biggest privacy risks or issues in "Big Data" and data analytics?
Includes Privacy Enhancing Technologies (PET), Privacy in Practice, Web Technology,	Q: Have you, or how would you incorporate privacy enhancing technologies into a System Development Lifecycle (SDLC)
ystems Lifecycle	Q: What types of issues can become barriers or cause friction between cybersecurity and privacy organizations? What experience have you had in this situation and how have you worked to overcome any friction?
	Q: What do you see as the potential privacy and security concerns with emerging geo-location technology in items such as "smart" clothing, smart homes, and smart chips for pets?
	Q: What are the main challenges with addressing privacy concerns in website or mobile application development? How would you, or have you, embedded privacy controls into website or app development?
	Q: Privacy needs to be embedded throughout the information lifecycle. Provide examples of privacy controls that you have implemented or that you feel should be implemented at the end of the information lifecycle, when information should be archived, retained or destroyed.

Minimization	Q: How does your organization define "sensitive PII"?
Includes Minimization of PII, Minimization of PII Used in Testing, Training and Research, and Data Retention and Disposal, Inventory of Personally Identifiable Information	Q: Does your organization have a PII inventory, and if so, how was it created and how is it maintained?
	Q: Please describe efforts you have taken in your work to minimize collection and retention of PII.
	Q: What questions or issues would you raise with a person who brings you a project that would involve collection and processing of sensitive PII?
	Q: What is the value of an inventory of personally identifiable information? Please explain how you have helped develop or maintain such an inventory.
	Q: What is anonymizing data, and how does that differ from de-identifying data? How would you guide an organization in anonymizing or de-identifying data it plans to share with a third party?
Use Limitation	Q: Describe how you interpret the requirements to share
Includes Internal Use	information internally only with those who "need to know" the information, and the processes put in place to implement this requirement.
	Q: What measures have you helped implement to ensure that PII is only shared externally as authorized?
Policy Analysis and Development Includes <i>Monitor and Analyze</i> <i>Privacy Law and</i> Policies.	Q: Have you written information security policy? What are the similarities between Information security and privacy policy and what are the difference?
	Q: What are some of the most effective privacy or security policies you have read? What elements made them effective?
	Q: Explain the difference between answering a question with "what is legally acceptable" vs. "what is the right thing to do?" Have you faced this question in your work?
	Q: Describe privacy-related policies you have drafted or had input into, and any challenges you faced in drafting, organizational adoption of the policy, or implementation.
	Q: [If the agency collects and maintains data from the EU] Please explain your familiarity if any with the EU General Data Protection Regulation (GDPR). If familiar with the GDPR, what do you see as the most significant impacts of the GDPR on U.S. organizations, public and private sector, and particularly in information security?

Privacy Advice and Guidance	Q: Your responsibility includes supporting the organization's business operations by advising on privacy requirements. Explain scenarios where you have advised other employees on privacy requirements, your approach, what worked well, and what challenges you faced.
	Q: How do you measure the success of a privacy program/policy? What metrics might be important to collect and review?
	Q: Tell me about a time you influenced others to re-think a business approach because it raised significant privacy risks?
Privacy Awareness and Training/ Technology Awareness	Q: Describe situations where you have had to train other individuals.
	Q: How are your organization's on-boarding and annual privacy and security training programs handled, and what are the key topics in those programs?
	Q: What has been your most effective staff awareness activity?
	Q: In addition to annual training, what other types of privacy and security training does your organization provide and how are you involved?
	Q: <i>[senior level position]</i> Describe the types of privacy and security training you have delivered, the audience for that training, and any reactions or outcomes you recall from the training.
	Q: [mid to senior level position] What format of training have you found to be most effective?
Continual Learning (General Competency)	Q: How do you keep up with changes to privacy and security laws, policies and standards?
	Q: What was the last training or privacy or security program you attended?

Privacy Impact and Risk Assessment Includes Privacy Risk	Q: What are some of the most effective privacy or security policies you have read? What elements made them effective?
Management/ATOs, Risk Management, Privacy by Design, Vulnerability Assessment	Q: Explain the difference between answering a question with "what is legally acceptable" vs. "what is the right thing to do?"
	Q: What do you think are the top three privacy risks in most Government Agencies?
	Q: What is a Privacy Impact Assessment (PIA) and when should a PIA be performed?
	Q: What are the benefits of a privacy specialist reviewing and approving a PIA, rather than leaving it up to the IT group or others?
	Q: Please explain the types of risks you have identified in conducting PIAs and how you have mitigated those risks.
	Q. Provide examples of the privacy controls described in NIST Spec. Pub. 800-53, Revision 4, and tell us your experience in developing, implementing and assessing the effectiveness of privacy controls.
	Q: How do you feel the NIST SP 800-52 Appendix J Privacy Controls align with the rest of the NIST SP 800-53 controls? How have you or would you implement those controls effectively?
	Q: What do you see as differences between information security and information privacy? And how are they aligned?
	Q: How have you, or would you, implement "privacy by design" (PbD)? How would you gain access to the system developers to influence them to adopt PbD standards in the system development lifecycle? What obstacles have you encountered in your organization in implementing PbD?

Privacy Incident Response Includes Incident Management	Q. In your own words, what is a PII data breach, and as the privacy specialist what would you want to know about such a breach?
	Q: Have you ever been involved in helping respond to a breach of personal data or other data security incident? Describe your experience and role, if any, in investigating the breach or other incident, providing notice to affected individuals, determining what steps should be taken to mitigate the breach or incident, developing strategies for avoiding similar breaches or incidents in the future, other lessons learned.
	Q: What is the importance of notification of affected individuals when data breaches occur?
	Q: Explain any experience you have had in notifying appropriate government authorities about a data breach.
Information Sharing With Third Parties Includes Privacy Requirements for Contractors and Service Providers, Contract and Grant	Q: Describe your experience with retaining and using contractors that handle or process PII, or if you have not had this experience, what issues would you expect to address? What actions have you taken, or would you take, to ensure that PII is sufficiently protected?
Oversight	Q: One significant vulnerability all organizations face is ensuring that their service providers protect data to which they have access. Describe your experience addressing this vulnerability and how you suggest these risks be minimized.
	Q: How would you assess third parties who handle PII on the organization's behalf?
	Q: Describe ways that you could assure yourself that a service provider is actually doing what it says it is doing.
	Q: Are there privacy concerns with cloud storage technology? Does your organization use cloud technology, if so how are any privacy concerns addressed?
Privacy Reporting	Q: Have you participated in providing written reports to your senior staff, Congress, OMB or other government agencies (or if private sector, your Board of Directors)?
	Q. What is FISMA and how does FISMA apply to Privacy?
	Q. What are Privacy Controls as described in NIST (800-53, Appendix J rev4), and tell us your experience in assessing Privacy Controls in your organization?

Data Quality and Integrity Includes Information Assurance	Q. Define data quality and what distinguishes data quality from data integrity? Why is this distinction important to understand?
	Q: What are some ways an organization can help ensure data quality and integrity?
	Q: What technical measures would you look for to ensure that data integrity is maintained?
	Q: Describe difficulties you have faced when performing in an information assurance role, i.e., reviewing or auditing controls to ensure appropriate protection of information and information systems. How did you overcome those difficulties?
Project Management	Q: Describe situations where you have managed projects. What went well, what were the challenges, and did you accomplish your goals?
Privacy Monitoring and Auditing	Q: How would you address gaps in privacy processes within an organization?
	Q: You have been tasked to conduct a privacy compliance review and present some recommendations to the organization about how PII data is handled. The organization is led by a senior executive who collects sensitive information from and about the public. There is room for improvement in how public information is collected, managed, accounted for and secured. How would you approach this project in terms of tasks and major considerations?
Dissemination of Privacy Program Information, Privacy Advice and Guidance	Q: Your responsibility includes supporting the organization's (business operations, project launches, new systems and applications,) by advising on Privacy requirements. How would you perform that role?
	Q: How do you measure the success of a privacy program/policy? What metrics might be important to collect and review?

Security Includes inventory and incident response, Communications Security Management, Computer Network Defense Information Systems/Network Security) Computer Network Defense , Information Systems Security Certification	 Q: What are the challenges of cloud computing with data protection and data integrity? How does an organization ensure that the appropriate level of cloud data security is available for the types of data to be stored in the cloud? Have you relied on FedRAMP in your current role? Q: Why is a system data breach both a cybersecurity and privacy concern, please elaborate? Q: What do you see as the biggest challenges in practicing privacy within a security or IT organization? What do you see as the benefits?
Data Management/Encryption/Identity Management	 Q: What experience have you had using different identifiers to identify individuals? Q: What encryption controls would you implement for Social Security Numbers? Do you have experience with encrypting data at rest? Data in motion? What encryption techniques or approaches do you find most successful in actually protecting data?
Enterprise Architecture Includes Operating Systems, Configuration Management, Information Resource Strategy and Planning, and Hardware	 Q: How has your organization planned (is your organization planning) to implement revised OMB Circular A-130? What will be the most significant changes for how your program has been operating? Q: Please describe examples of privacy controls that can be embedded into operating systems and also system architecture.
Senior Level Positions: Governance and Privacy Program Includes Program Management, Developing Others, Leadership	 Q: What are some of the primary responsibilities of an organization's privacy program? Q: What do you view as the most effective organizational governance structure of a privacy program within an organization, e.g., reporting relationships? Q: Please describe your experience developing and implementing budgets. What key lessons have you learned from your experience? Q: Privacy leaders often dream of implementing the ideal privacy program, but the reality is often that the resources are not available. How would you manage a privacy program to make the most of the resources you have?

Supervisory Positions:	Q: Explain your experience in workforce planning. Are you
Workforce Planning	familiar with the parts of OMB revised Circular A-130 regarding workforce planning, and if so, how would you
Includes Managing Human	meet those requirements?
<i>Resources, Developing Others, Employee Development</i>	Q: Please describe your experience managing other employees, including how you have developed employees.
	Q: What key lessons have you learned in your experience as a manager?