



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

NOV 01 2016

PERSONNEL BULLETIN NO: 16-12

SUBJECT: Standardized Position Descriptions for Bureau Associate Privacy Officers

- 1. Purpose.** The bulletin establishes Department of the Interior standard position descriptions (SPDs) for supervisory and non-supervisory Bureau Associate Privacy Officer (APO) positions at the GS14 and GS15 levels.
- 2. Background.** The SPDs are part of the Department's implementation of the Federal Information Technology Acquisition Reform Act (FITARA), specifically supporting requirements related to the enhancement of hiring, performance management and workforce planning within information management and technology programs. The Department's Office of Human Resources (OHR) and Office, Chief Information Officer (OCIO) collaborated to establish these SPDs. The OCIO provided a copy of the SPDs to bureau information management teams via email.
- 3. Policy.** Bureau human resource offices should work with appropriate offices to ensure all APOs are on the appropriate SPD by Friday, December 30, 2016. The official SPDs with SPD numbers covered by this Personnel Bulletin are:

Government Information Specialist, GS-0306-14	(SPD Number DOII001)
Supervisory Government Information Specialist, GS-0306-14	(SPD Number DOII002)
Government Information Specialist, GS-0306-15	(SPD Number DOII003)
Supervisory Government Information Specialist, GS-0306-15	(SPD Number DOII004)

4. Position Titles:

Official Titles. In accordance with the law (5 U.S.C. 5105), the U.S. Office of Personnel Management (OPM) must establish official titles for positions based on the occupational series assigned. These prescribed titles are specified in published classification standards. Titles are based on their occupational series and any specialized function it performs (i.e., Government Information Specialist). These titles must be coded into FPPS and be reflected on the incumbents' SF-50, *Notification of Personnel Action*. The official titles assigned to the APO SPD follows the OPM standards for the GS-0306 series.

Organizational Titles. In addition to the official title, the agency has the option to assign an organizational title that reflects the position's organizational placement or specific program focus. For example, a position classified as a GS-0306-14 may have an official title of Supervisory Government Information Specialist and an organizational title of Associate Privacy Officer. The organizational title assigned to the above SPDs is Associate Privacy Officer.

5. Standard PD Numbering System. Bureaus/Offices must implement the DOI SPD numbering system for newly established positions when replacing existing PDs with the standard ones. The DOI SPD number must be entered into FPPS, in accordance with Bureau procedures, so it prints on the incumbent's SF-50 (Notification of Personnel Action). The SPD number is recorded in Block 1 of the OF-8 attached for each DOI SPD. In order to conform with the position number data field length in FPPS, the SPD numbers assigned are seven digits in length.

6. Management's Responsibility for PD Accuracy and Position Management. Use of Standardized PDs in no way detracts from management's authority and responsibility to ensure that officially assigned and performed duties and responsibilities accurately match PDs of record for all covered employees. Likewise, using SPDs also does not diminish management's responsibility to adhere to basic position management principles. Management officials are urged to contact their respective servicing human resources office for classification and position management advice and guidance.

7. Exception to the Rules. Bureaus may make some updates to these SPDs to reflect bureau-specific requirements. However, major changes that will alter the classification and/or grades of the positions must be avoided. Bureau Human Resource Offices and Associate Chief Information Officers must fully coordinate any changes to these SPDs.

Questions concerning SPDs should be directed to the respective Bureau/equivalent Human Resources Office. The DOI, Office of Human Resources contact is Martin Pursley at martin_pursley@ios.doi.gov.



Raymond A. Limon
Director, Office of Human Resources

POSITION DESCRIPTION (Please Read Instructions on the Back)

1. Agency Position No.
DOII001

2. Reason for Submission <input type="checkbox"/> Redescription <input checked="" type="checkbox"/> New <input type="checkbox"/> Reestablishment <input type="checkbox"/> Other Explanation (Show any positions replaced)		3. Service <input checked="" type="checkbox"/> Hdqtrs <input type="checkbox"/> Field		4. Employing Office Location		5. Duty Station		6. OPM Certification No.	
7. Fair Labor Standards Act <input checked="" type="checkbox"/> Exempt <input type="checkbox"/> Nonexempt				8. Financial Statements Required <input type="checkbox"/> Executive Personnel Financial Disclosure <input type="checkbox"/> Employment and Financial Interest		9. Subject to IA Action <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No			
10. Position Status <input type="checkbox"/> Competitive <input type="checkbox"/> Excepted (Specify in Remarks) <input type="checkbox"/> SES (Gen.) <input type="checkbox"/> SES (CR)				11. Position Is <input type="checkbox"/> Supervisory <input type="checkbox"/> Managerial <input checked="" type="checkbox"/> Neither		12. Sensitivity <input type="checkbox"/> 1--Non-Sensitive <input type="checkbox"/> 3--Critical <input type="checkbox"/> 2--Noncritical Sensitive <input type="checkbox"/> 4--Special Sensitive		13. Competitive Level Code	
14. Agency Use									

15. Classified/Graded by	Official Title of Position	Pay Plan	Occupational Code	Grade	Initials	Date
a. Office of Personnel Management						
b. Department, Agency or Establishment						
c. Second Level Review	Government Information Specialist	GS	0306	14		
d. First Level Review						
e. Recommended by Supervisor or Initiating Office						

16. Organizational Title of Position (if different from official title)
Associate Privacy Officer

17. Name of Employee (if vacant, specify)

18. Department, Agency, or Establishment Department of the Interior		c. Third Subdivision	
a. First Subdivision		d. Fourth Subdivision	
b. Second Subdivision		e. Fifth Subdivision	
f. Employee Review-This is an accurate description of the major duties and responsibilities of my position.		Signature of Employee (optional)	

20. **Supervisory Certification.** I certify that this is an accurate statement of the major duties and responsibilities of this position and its organizational relationships, and that the position is necessary to carry out Government functions for which I am responsible. This certification is made with the knowledge that this information is to be used for statutory purposes relating to appointment and payment of public funds, and that false or misleading statements may constitute violations of such statutes or their implementing regulations.

a. Typed Name and Title of Immediate Supervisor		b. Typed Name and Title of Higher-Level Supervisor or Manager (optional)	
Signature	Date	Signature	Date

21. Classification/Job Grading Certification. I certify that this position has been classified/graded as required by Title 5, U.S. Code, in conformance with standards published by the U.S. Office of Personnel Management or, if no published standards apply directly, consistently with the most applicable published standards.		22. Position Classification Standards Used in Classifying/Grading Position	
Typed Name and Title of Official Taking Action Martin Pursley Director, Talent Management		Information for Employees. The standards, and information on their application, are available in the personnel office. The classification of the position may be reviewed and corrected by the agency or the U.S. Office of Personnel Management. Information on classification/job grading appeals, and complaints on exemption from FLSA, is available from the personnel office or the U.S. Office of Personnel Management.	
Signature	Date 11/25/16		

23. Position Review	Initials	Date	Initials	Date	Initials	Date	Initials	Date	Initials	Date
a. Employee (optional)										
b. Supervisor										
c. Classifier										
Remarks										

25. Description of Major Duties and Responsibilities (See Attached)

**Department of the Interior
Government Information Specialist
GS-0306-14**

Organizational Title: Associate Privacy Officer

Introduction

This position is for the Department of the Interior (DOI or Department) [bureau/office] Associate Privacy Officer (APO) located in [bureau/office] (bureau). The APO reports directly to the [bureau] Associate Chief Information Officer (ACIO) and is responsible for planning, developing, analyzing, evaluating and administering the Bureau Privacy Program, to include policy and training development, the execution, administration and conduct of the program, oversight of privacy program functions, providing guidance on privacy-related matters, implementing and assessing privacy activities, and establishing plans and strategies for implementing privacy and data protection initiatives. The APO also reports to the Departmental Privacy Officer (DPO) for privacy program compliance activities, and provides collaboration and support for agency privacy program functions. The APO serves as the Bureau privacy subject matter expert and focal point for privacy issues, has Privacy Act oversight and reporting responsibility, and provides guidance and recommendations to Bureau-level senior officials on the implementation of the Department's privacy priorities and plans. The position requires expert technical, research, and analytical skills, to include mastery in interpretation of the Privacy laws and policies. Additionally, incumbent must have superb judgment and have the ability to make sound decisions and provide guidance to top-level Bureau officials.

The primary responsibility of the APO is to provide privacy program advocacy, oversight, leadership and guidance for their Bureau in coordination with the DPO and in alignment with the DOI Privacy Program. The APO must have comprehensive knowledge and understanding of Federal privacy laws and regulatory and policy requirements, and ensures that all Bureau privacy activities adhere to the requirements of the Privacy Act of 1974, the Computer Matching and Privacy Protection Act, the E-Government Act of 2002, the Federal Information Security Modernization Act, the Electronic Communications Privacy Act, the Intelligence Reform and Terrorism Prevention Act of 2004, the Health Insurance Portability and Accountability Act (HIPAA) where applicable, Office of Management and Budget (OMB) directives, National Institute of Standards and Technology (NIST) standards and guidance, DOI Privacy Act and privacy program regulations and policies, and other applicable laws, policies, and standards. The APO ensures privacy laws, regulations and policies are implemented and a privacy framework is established for the protection of information privacy.

Major Duties

Privacy Leadership

The APO is responsible for full Bureau Privacy Program management, leads Bureau Privacy

Program activities, and is the primary point of contact with the Departmental Privacy Officer, Federal, Tribal, state and local government offices, organizations, and the public in addressing privacy issues.

- Represent the Bureau on activities and requirements of the Privacy Act, privacy provisions of the E-Government Act, Intelligence Reform and Terrorism Prevention Act, and related Federal privacy laws, regulations, and policies.
- Represent Bureau interests and participates on intra-Agency, inter-Agency, and inter-governmental committees and task-forces.
- Serve as liaison and subject matter expert on Bureau privacy complaints, issues, and problems to assist and advise Bureau management, employees, and contractors regarding resolution of problems and privacy-related issues.
- Lead the Bureau Identity Theft Task Force and oversee Bureau privacy incident response activities to mitigate the impact of privacy incidents on individuals and the agency, provide internal and external notifications as necessary, and ensure appropriate reporting to internal and external organizations in coordination with the Departmental Privacy Officer.
- Develop lessons learned, updates Bureau privacy policies and strategies, and provides briefings and reports to Bureau leadership and the Departmental Privacy Officer.
- Address Bureau privacy program deficiencies with Bureau leadership and the Departmental Privacy Officer to improve program functions and maintain compliance with Federal and Departmental privacy requirements.
- Evaluate the effectiveness of Bureau privacy policies and practices, and establish plans and strategies to identify ways to mitigate gaps and obtain objectives.
- Develop and provide privacy training, orientation tools and resources for different levels of employees (and contractors) based on roles and responsibilities, as well as specific needs and skill development.
- Provide guidance and prepare responses to privacy questions from Bureau officials, and prepare responses to privacy-related inquiries from the Department and other internal and external oversight organizations including Office of Inspector General, Office of Management and Budget, and Congress.
- Initiate appropriate action and oversee privacy complaints in coordination and collaboration with the Department, Bureau and program officials, and legal counsel when necessary.
- Coordinate with senior management, legal counsel, and other parties to represent the Bureau information privacy interests with internal and external parties on proposed new or amended legislation, regulations, or policies, as well as on audits or reviews of privacy functions or program areas with privacy implications.

Policy Development

The APO oversees the development, implementation, maintenance of, and adherence to Bureau policies and procedures covering the collection, handling, safeguarding, sharing and disclosure of personally identifiable information in compliance with Federal laws, Departmental regulations, and privacy policies.

- Develop, update and implement 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.
- Review, analyze and/or develop proposed rulemakings, regulations, guidelines or other documents to determine privacy impacts, communicating those impacts to the appropriate Departmental or Bureau officials, working with program officials to revise proposed policy, rulemaking or other documents to address privacy implications and mitigate risks.
 - Review and analyze bureau policies or bureau manual chapters, proposed policy guidance, related documents pertaining to Privacy Act systems of records, and any associated rulemaking documentation for effect on Bureau mission and program activities.
 - Provide guidance and interpretation, and assist in the implementation and maintenance of Departmental privacy policies related to the Privacy Act, E- Government Act privacy provisions, Intelligence Reform and Terrorism Prevention Act of 2004, OMB guidance, NIST standards, and related laws, policies and procedures.
 - Collaborate with information resource management officials to incorporate privacy requirements and best practices in coordination with Bureau senior staff and managers.
 - Develop and implement processes and initiatives to assess privacy risk in Bureau information systems, websites, programs, projects, information collections, social media, and new technologies.
 - Develop and implement strategies and plans for the implementation of privacy protection policy and practices across the Bureau throughout the information life cycle in order to meet Federal government compliance requirements and standards for privacy protection in information systems.

Privacy Compliance and Oversight

Oversee and manage Bureau privacy program activities including, but not limited to, compliance with the Privacy Act of 1974, the E-Government Act of 2002, Federal Information Security Modernization Act (FISMA), Intelligence Reform and Terrorism Prevention Act of 2004, Health Insurance Portability and Accountability Act (HIPAA), the Electronic Communications Privacy Act, Government Paperwork Elimination Act, Information Protection and Security Act, Identity Theft Prevention Act, Online Privacy Protection and Security Act, Social Security Number Protection Act, OMB Circular A-130 and privacy policies, National Institute of Standards and Technology guidance and standards in coordination with the Departmental Privacy Officer.

- Monitor and analyze privacy laws and requirements, and effectively communicate requirements in writing and orally to other staff.
- Advise and provide guidance to staff to mitigate privacy related risks and ensure compliance with privacy requirements.
- Develop and implement processes and procedures to review proposed data collections in the early stages of the Bureau's decision-making process; and ensure the program office has legal authority to collect the information and only collects PII relevant and necessary to support the mission.
- Maintain and regularly update the bureau's inventory of PII holdings, and work with Bureau officials to minimize the unnecessary collection, use and holdings of Social Security numbers and PII, and report status of PII holdings to the Departmental Privacy

- Officer in accordance with Federal government mandates and Departmental policy.
- Collaborate with Bureau officials to conduct reviews of PII within the Bureau and with contractors, partners and third parties to ensure ongoing compliance with the Privacy Act and related privacy laws and policies, that appropriate controls are implemented to safeguard PII, memorandums of understanding and agreements are reviewed for adequacy as required to protect privacy, and information sharing activities are conducted in accordance with applicable laws and policies.
 - Conduct reviews of prospective contractors or grantees to ensure they can meet privacy requirements, ensure privacy requirements are included in contract, acquisition or grant-related documentation, and audits/reviews for compliance with privacy requirements are conducted regularly during the period of performance.
 - Prepare reports to the Office of Management and Budget, Congress, other oversight body and organizations as needed in coordination with the Departmental Privacy Officer, including but not limited to Senior Agency Official for Privacy Reports under FISMA, reports on computer matching, reports on information sharing environment activities as required, etc. to demonstrate accountability and transparency of organizational privacy operations.
 - Oversee completion of mandatory annual and role-based privacy training and privacy awareness campaigns efforts by drafting privacy training and awareness plans. Develop privacy awareness communications and deliver targeted role-based training for staff handling PII when needed, and maintain Bureau privacy program information on public websites and Bureau intranet sites as needed to promote employee awareness of privacy requirements and responsibilities.
 - Ensure Bureau policies and practices are in compliance with laws, regulatory requirements and Departmental privacy program strategies, procedures and standards.
 - Review proposed privacy policies and monitor current policy to ensure implementation and privacy issues are adequately addressed (e.g., Privacy Impact Assessments are completed for Information Technology initiatives).
 - Conduct management evaluations and internal control processes to ensure ongoing compliance monitoring of the Bureau privacy program.
 - Ensure compliance with privacy practices and take appropriate action to correct deficiencies or failure to comply with privacy policies for the Bureau employee extended workforce, contractors, partners and business associates, in consultation with Human Resources, Bureau leadership, administration, and legal counsel.
 - Develop metrics to measure the Bureau's privacy performance, develop strategies for improvement and report findings and recommendations to Bureau management and the Departmental Privacy Officer.
 - Provide reports on status of Bureau privacy program activities as required by the Departmental Privacy Officer.

Privacy Analysis and Assessment

Analyzes privacy source systems, databases, projects, and information collections, conducts reviews, and updates privacy compliance documentation in support of the Department in accordance with privacy laws, regulations and policies.

- Maintain Bureau System of Records Notices (SORNs) for records maintained in paper,

micro, or electronic format (or a combination of these formats) that contain records about individuals in accordance with the provisions of the Privacy Act of 1974. Work with system managers to review and update SORNs, and support Departmental Privacy Officer review and approval process for SORN publication in the Federal Register.

- Ensure Privacy Impact Assessments are conducted as required for information systems, projects, information collections developed within the Bureau in accordance with Departmental policy requirements.
- Develop and update privacy notices and Privacy Act Statements for information collections from individuals, and ensure that the purpose for collection is specified in privacy notices, individuals are provided an opportunity to consent to data collection when appropriate, individuals are advised of how to access and correct information about them, and how to contact the Bureau for privacy complaints.
- Prepare responses to questions from employees about handling PII, privacy risks, ways to improve business processes or otherwise mitigate risks, and meet legal and policy requirements.
- Coordinate and implement privacy requirements, policies and procedures, with records management, FOIA, information collection clearance, security and other information management functions.
- Develop and implement processes and procedures to conduct privacy review of proposed new data collections early in the agency's decision-making process, and analyze how PII is handled in current and new technologies, identifying risks utilizing methods and tools used for risk assessment, and advising personnel on ways to mitigate risks.
- Assist in developing and implementing technologies, principles and processes to analyze, prioritize and respond to incidents involving compromise or unauthorized disclosure or access to PII, and regularly review incidents to understand patterns and develop mitigation measures.
- Analyze privacy risks and ensure implementation of privacy controls (including privacy continuous monitoring strategies and controls stated in NIST SP 800-53 Rev. 4, App. J "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 program officials, security, and the Departmental Privacy Officer.

Performs other related duties and responsibilities as assigned.

Factor Level Descriptions

Factor 1. Knowledge Required by the Position: Level 1-8, 1550 Points

Mastery of and skill in applying a wide range of qualitative and quantitative methods for the assessment and improvement of complex privacy related programs, processes and systems, including the sequence and timing of key privacy and security program milestones, and methods to evaluate the worth of the Bureau program accomplishments, as they relate to management of planned privacy program objectives.

Mastery knowledge of a wide range of administrative laws, policies, regulations and precedents including OMB and Department regulations applicable to the administration of the Bureau-wide privacy program sufficient to improve processes, make recommendations to senior management, and provide oversight of the privacy program.

Expert knowledge in the areas of Privacy policy analysis and development, Privacy program development and implementation, information law and disclosure issues, Departmental privacy guidance and compliance programs, employee privacy issues, legislative issues affecting privacy, and various privacy publications sufficient to represent the Bureau.

Comprehensive knowledge of the Privacy Act, OMB guidance, the Computer Matching and Privacy Protection Act, E-Government Act, FISMA, HIPAA, privacy statutory, regulatory and other legal requirements for privacy policy and its application to information resource management, Department policies, and other areas of privacy law in order to meet responsibilities for Bureau compliance initiatives regarding these laws, regulations, and policies.

In-depth knowledge and experience in gathering, assembling, interpreting and analyzing a vast amount of complex privacy and security related technical data and materials, including identifying key issues, drawing sound conclusions and developing authoritative recommendations, approaches and comprehensive management reports concerned with established and/or proposed privacy policies and plans.

Exceptional interpersonal, verbal and written communications skills, sufficient to prepare and present technical material, policy, regulations, guidance, briefing materials, and reports to management in support of the privacy program and in order to brief and guide staff and high level management during privacy breaches, privacy mitigation loss strategies, privacy task force(s) and associated responsibilities.

Demonstrated expert knowledge in conducting Privacy Impact Assessments on highly complex computer and information systems to ensure identification and protection of privacy information.

In-depth knowledge and understanding of the Bureau organizations and various functional operations to develop, implement, and evaluate privacy issues and management and the ability to provide innovative technical direction for resolution of critical problems anticipated in the accomplishment of privacy program requirements.

Expert knowledge of Privacy Act requirements to determine and evaluate the potential effects of privacy requirements on business operations and developing strategies to assist Bureau operations in meeting their privacy and legal policy requirements.

Incumbent must possess high degree of professionalism in demonstrating and applying discretion and judgment when dealing with sensitive issues.

Requires skill in handling criticisms of Bureau performance, to logically and effectively explain

issues, programs, functions and activities, providing a better understanding of the organization's efforts to concerned public citizens.

DESIRED: Obtain and maintain at least one of the following privacy professional certifications from the International Association of Privacy Professionals: Certified Information Privacy Professional/US Government (CIPP/G); Certified Information Privacy Manager (CIPM)

Factor 2. Supervisory Controls: Level 2-5, 650 Points

The incumbent works under the general supervision of the Bureau Associate Chief Information Officer and in close collaboration with the Departmental Privacy Officer, with responsibility for meeting Bureau and Departmental level privacy objectives. As a recognized authority and privacy subject matter expert, the incumbent is responsible for the evaluation of privacy program functions and issues, and is subject only to administrative and policy direction concerning overall project priorities and objectives. The incumbent is delegated authority to independently plan, schedule, implement and monitor major projects concerned with the analysis and evaluation of the effectiveness of the Bureau privacy program and privacy initiatives, and communicating pertinent information relative to the Bureau privacy program activities. Analyses, evaluations and recommendations developed by the employee are normally reviewed by management officials only for potential influence on broad agency policy objectives and program goals. Supervision is generally in terms of broad policy and program direction and the incumbent must have the ability to produce and is subject to a high degree on the incumbent's ability to produce and develop high quality actions and recommendations independently. Incumbent initiates and participates in the development of objectives to be accomplished relating to Federal government privacy requirements and privacy protection. The incumbent has wide latitude in establishing priorities, determining approaches and independently planning, designing and carrying out programs, projects, and studies. Determinations, recommendations, and conclusions are considered definitive. Work is reviewed on such matters as fulfillment of program objectives and mission accomplishments.

Factor 3. Guidelines: Level 3-5, 650 Points

Basic guidance may be found in Departmental policy, legislation and regulations that offer very broad operating parameters, including rapidly evolving guidance provided by oversight agencies such as the Office of Management and Budget (OMB), Government Accountability Office, Department of Justice, General Services Administration, and National Institute of Standards and Technology. State, local, and Tribal statutes must be considered as they might affect or be affected by proposed Federal policies. Incumbent may draft or initiate changes in regulations or Departmental policy for consideration and approval by the DPO. Incumbent must use high levels of originality, judgment, discretion and creativeness to interpret intent and applicability, to adapt to the changing requirements, and to meet customer needs and add value in the most efficient and cost-effective way possible. Guidelines include laws, regulations, Departmental manuals, handbooks, policies, standards, and program documents, other legal requirements of the Federal government and long-range plans. Also included is literature concerning privacy issues and materials dealing with computer technology, organization, management, and evaluation techniques.

The incumbent identifies the need for and develops management and administrative policies, procedures, guidelines, and privacy protection tools needed to ensure compliance with the Privacy Act of 1974, E-Government Act, FISMA, HIPAA, the Intelligence Reform and Terrorism Prevention Act, the Electronic Communications Privacy Act, Government Paperwork Elimination Act, Information Protection and Security Act, Identity Theft Prevention Act, Online Privacy Protection and Security Act, Social Security Number Protection Act, non-disclosure statutes, OMB Circular A-130, OMB policy, NIST standards, Federal Information Processing Standards, specifically FIPS-199, user authentication, and related Federal privacy laws, policy and guidelines.

Factor 4. Complexity: Level 4-5, 325 Points

The incumbent analyzes interrelated issues to determine effectiveness, efficiency, and productivity for Bureau-wide privacy administrative and operational privacy programs. The incumbent develops detailed plans, goals, and end objectives for long-range implementation and administration of the privacy policies, plans and management initiatives. The incumbent develops criteria for evaluating the effectiveness of the privacy program. Decisions concerning planning, organizing and conducting studies are complicated by conflicting laws, program goals and objectives, and the incumbent must ensure that privacy program requirements are met in a way that allows organization mission goals to be completed.

Assignments related to privacy violations may be complicated by the need to deal with subjective concepts, sensitive situations, and combative or defensive parties. Most privacy issues are complex and unique so findings and conclusions may be highly subjective and not readily susceptible to verification through replication of study methods or reevaluation of results. Options, recommendations, and conclusions take into account and give appropriate weight to interpretation of privacy regulations, foreseeable harm to the organization and individuals, severity of events, and a wide range of other variables which affect long-range privacy program performance and direction.

Factor 5. Scope and Effect: Level 5-5, 325 Points

The purpose of the work is to analyze and evaluate privacy implications and protections for major administrative aspects of substantive, mission-oriented programs. This may involve, for example, the development of long-range program plans, goals, objectives, and milestones or evaluating the effectiveness of programs conducted throughout the Bureau. The Bureau's activities greatly affect the general public and the Bureau's activities are subject to constant controversy and scrutiny from all sources, including the national and local news media, and various interest groups. Privacy is highly visible and compliance with privacy laws and policies is critical to the Bureau's mission. Without appropriate privacy controls in place to safeguard privacy, compromise of government systems and data can have significant impact on individuals, and can affect public confidence and the agency's mission.

Factor 6, Personal Contacts and Factor 7, Purpose of Contacts: Level 3c, 180 Points

Personal Contacts:

Extensive personal contacts are required with executive officials, professional, technical, administrative, and managerial personnel, throughout the Bureau, the Office of the Chief Information Officer, Office of Regulatory Affairs, Office of Policy Analysis and Office of the Solicitor, and staffs at other Bureaus/Offices and at different organizational levels of the Department. Contacts may also be required with the Office of Federal Register, OMB, Federal, state agencies, tribal governments, private industry, and environmental groups. Incumbent has direct liaison with officials from Government-wide committees and working groups, Inter-Governmental organizations, Congressional representatives, law firms, and members of the general public, as well as liaison and collaboration with representatives of stakeholder groups and senior Federal officials.

The incumbent maintains regular contact with interested national and local professional organizations, industry and interest groups, and other non-governmental organizations. Communication with contacts are made through standing coordination meetings, working groups, presentations, personal contact, by telephone, paper or electronic correspondence or any combination of these methods, when such contacts occur on an ad hoc basis.

Purpose of Contacts:

Contacts with the Department, other governmental and non-governmental offices are made to plan, coordinate, advise, secure, direct or influence others regarding significant issues and to resolve problems of mutual concern and ensuring that Privacy Act activities are consistent with legal precedent and policy. The incumbent must represent the Bureau's position on various planning process aspects concerning privacy within and outside the Department. The incumbent proposes solutions and mediates differing objectives into mutually beneficial courses of action to gain acceptance of ideas or to achieve compliance with established privacy policies and regulations.

Contacts with Bureau internal program offices are largely to conduct privacy assessments, evaluate privacy controls and ensure compliance, resolve privacy issues and complaints, perform investigations on incidents, provide privacy program information, training, and guidance, and promote awareness. These contacts also are made to maintain knowledge of current mission objectives, information systems and initiatives, and other program activities as they relate to privacy issues. The incumbent must explain privacy policy positions and make recommendations, and negotiate differences in matters concerning privacy program responsibilities and mission objectives. The incumbent must frequently present and defend analyses and recommendations in meetings with individuals and organizations with conflicting priorities. The incumbent may negotiate matters and may make commitments within his/her area of responsibility.

Public contacts usually involve coordination 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 8. Physical Demands: Level 8-1, 5 Points

The work is mostly sedentary. Some travel is required, both within and outside the local commuting area. Occasional travel may be required to field activities for compliance review, determination of activity performance, and to conduct training and/or technical assistance. The incumbent must be able to function well under stressful conditions, often working under very tight deadlines involving projects of national significance.

Factor 9. Work Environment: Level 9-1, 5 Points

Work is performed primarily in office areas, conference rooms, and similar environments. No hazardous conditions are anticipated.

TOTAL POINTS = 3690 = GS-14

POINT RANGE = 3605-4050

POSITION DESCRIPTION (Please Read Instructions on the Back)

1. Agency Position No.
DOI1002

2. Reason for Submission <input checked="" type="checkbox"/> Redescription <input checked="" type="checkbox"/> New <input checked="" type="checkbox"/> Hdqtrs <input type="checkbox"/> Field <input type="checkbox"/> Reestablishment <input type="checkbox"/> Other	3. Service	4. Employing Office Location	5. Duty Station	6. OPM Certification No.
Explanation (Show any positions replaced)		7. Fair Labor Standards Act <input checked="" type="checkbox"/> Exempt <input type="checkbox"/> Nonexempt	8. Financial Statements Required <input type="checkbox"/> Executive Personnel Financial Disclosure <input type="checkbox"/> Employment and Financial Interest	
		9. Subject to IA Action <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No		

10. Position Status <input type="checkbox"/> Competitive <input type="checkbox"/> Excepted (Specify in Remarks) <input type="checkbox"/> SES (Gen.) <input type="checkbox"/> SES (CR)	11. Position Is <input checked="" type="checkbox"/> Supervisory <input type="checkbox"/> Managerial <input type="checkbox"/> Neither	12. Sensitivity <input type="checkbox"/> 1--Non-Sensitive <input type="checkbox"/> 3--Critical <input type="checkbox"/> 2--Noncritical Sensitive <input type="checkbox"/> 4--Special Sensitive	13. Competitive Level Code
			14. Agency Use

15. Classified/Graded by	Official Title of Position	Pay Plan	Occupational Code	Grade	Initials	Date
a. Office of Personnel Management						
b. Department, Agency or Establishment						
c. Second Level Review	Supervisory Government Information Specialist	GS	0306	14		
d. First Level Review						
e. Recommended by Supervisor or Initiating Office						

16. Organizational Title of Position (if different from official title)
Associate Privacy Officer

17. Name of Employee (if vacant, specify)

18. Department, Agency, or Establishment Department of the Interior	c. Third Subdivision
a. First Subdivision	d. Fourth Subdivision
b. Second Subdivision	e. Fifth Subdivision

19. Employee Review-This is an accurate description of the major duties and responsibilities of my position.

Signature of Employee (optional)

20. **Supervisory Certification.** I certify that this is an accurate statement of the major duties and responsibilities of this position and its organizational relationships, and that the position is necessary to carry out Government functions for which I am responsible. This certification is made with the knowledge that this information is to be used for statutory purposes relating to appointment and payment of public funds, and that false or misleading statements may constitute violations of such statutes or their implementing regulations.

a. Typed Name and Title of Immediate Supervisor	b. Typed Name and Title of Higher-Level Supervisor or Manager (optional)
Signature _____ Date _____	Signature _____ Date _____

21. Classification/Job Grading Certification. I certify that this position has been classified/graded as required by Title 5, U.S. Code, in conformance with standards published by the U.S. Office of Personnel Management or, if no published standards apply directly, consistently with the most applicable published standards.	22. Position Classification Standards Used in Classifying/Grading Position
Typed Name and Title of Official Taking Action Martin Pursley Director, Talent Management	Information for Employees. The standards, and information on their application, are available in the personnel office. The classification of the position may be reviewed and corrected by the agency or the U.S. Office of Personnel Management. Information on classification/job grading appeals, and complaints on exemption from FLSA, is available from the personnel office or the U.S. Office of Personnel Management.
Signature _____ Date 10/26/16	

23. Position Review	Initials	Date	Initials	Date	Initials	Date	Initials	Date	Initials	Date
a. Employee (optional)										
b. Supervisor										
c. Classifier										
Remarks										

25. Description of Major Duties and Responsibilities (See Attached)

Department of the Interior
Supervisory Government Information Specialist
GS-0306-14

Organizational Title: Associate Privacy Officer

Introduction

This position is for the Department of the Interior (DOI or Department) [bureau/office] Associate Privacy Officer (APO) located in [bureau/office] (bureau). The APO reports directly to the [bureau] Associate Chief Information Officer (ACIO) and is responsible for planning, developing, analyzing, evaluating and administering the Bureau Privacy Program, to include policy and training development, the execution, administration and conduct of the program, oversight of privacy program functions, providing guidance on privacy-related matters, implementing and assessing privacy activities, and establishing plans and strategies for implementing privacy and data protection initiatives. The APO also reports to the Departmental Privacy Officer (DPO) for privacy program compliance activities, and provides collaboration and support for agency privacy program functions. The APO serves as the Bureau privacy subject matter expert and focal point for privacy issues, has Privacy Act oversight and reporting responsibility, and provides guidance and recommendations to Bureau-level senior officials on the implementation of the Department's privacy priorities and plans. The position requires expert technical, research, and analytical skills, to include mastery in interpretation of the Privacy laws and policies. Additionally, incumbent must have superb judgment and have the ability to make sound decisions and provide guidance to top-level Bureau officials.

The primary responsibility of the APO is to provide privacy program advocacy, oversight, leadership and guidance for their Bureau in coordination with the DPO and in alignment with the DOI Privacy Program. The APO must have comprehensive knowledge and understanding of Federal privacy laws and regulatory and policy requirements, and ensures that all Bureau privacy activities adhere to the requirements of the Privacy Act of 1974, the Computer Matching and Privacy Protection Act, the E-Government Act of 2002, the Federal Information Security Modernization Act, the Electronic Communications Privacy Act, the Intelligence Reform and Terrorism Prevention Act of 2004, the Health Insurance Portability and Accountability Act (HIPAA) where applicable, Office of Management and Budget (OMB) directives, National Institute of Standards and Technology (NIST) standards and guidance, DOI Privacy Act and privacy program regulations and policies, and other applicable laws, policies, and standards. The APO ensures privacy laws, regulations and policies are implemented and a privacy framework is established for the protection of information privacy.

Major Duties

Privacy Leadership

The APO is responsible for full Bureau Privacy Program management, leads Bureau Privacy

Program activities, and is the primary point of contact with the Departmental Privacy Officer, Federal, Tribal, state and local government offices, organizations, and the public in addressing privacy issues.

- Represent the bureau on activities and requirements of the Privacy Act, privacy provisions of the E-Government Act, Intelligence Reform and Terrorism Prevention Act, and related Federal privacy laws, regulations, and policies.
- Represent bureau interests and participates on intra-Agency, inter-Agency, and inter-governmental committees and task-forces.
- Serve as liaison and subject matter expert on bureau privacy complaints, issues, and problems to assist and advise bureau management, employees, and contractors regarding resolution of problems and privacy-related issues.
- Lead the bureau Identity Theft Task Force and oversee bureau privacy incident response activities to mitigate the impact of privacy incidents on individuals and the agency, provide internal and external notifications as necessary, and ensure appropriate reporting to internal and external organizations in coordination with the Departmental Privacy Officer.
- Develop lessons learned, updates bureau privacy policies and strategies, and provides briefings and reports to bureau leadership and the Departmental Privacy Officer.
- Address bureau privacy program deficiencies with bureau leadership and the Departmental Privacy Officer to improve program functions and maintain compliance with Federal and Departmental privacy requirements.
- Evaluate the effectiveness of bureau privacy policies and practices, and establish plans and strategies to identify ways to mitigate gaps and obtain objectives.
- Develop and provide privacy training, orientation tools and resources for different levels of employees (and contractors) based on roles and responsibilities, as well as specific needs and skill development.
- Provide guidance and prepare responses to privacy questions from bureau officials, and prepare responses to privacy-related inquiries from the Department and other internal and external oversight organizations including Office of Inspector General, Office of Management and Budget, and Congress.
- Initiate appropriate action and oversee privacy complaints in coordination and collaboration with the Department, bureau and program officials, and legal counsel when necessary.
- Coordinate with senior management, legal counsel, and other parties to represent the bureau information privacy interests with internal and external parties on proposed new or amended legislation, regulations, or policies, as well as on audits or reviews of privacy functions or program areas with privacy implications.

Policy Development

The APO oversees the development, implementation, maintenance of, and adherence to bureau policies and procedures covering the collection, handling, safeguarding, sharing and disclosure of personally identifiable information in compliance with Federal laws, Departmental regulations, and privacy policies.

- Develop, update and implement 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.

- Review, analyze and/or develop proposed rulemakings, regulations, guidelines or other documents to determine privacy impacts, communicating those impacts to the appropriate Departmental or bureau officials, working with program officials to revise proposed policy, rulemaking or other documents to address privacy implications and mitigate risks.
- Review and analyze bureau policy or bureau manual chapters, proposed policy guidance, related documents pertaining to Privacy Act systems of records, and any associated rulemaking documentation for effect on bureau mission and program activities.
- Provide guidance and interpretation, and assist in the implementation and maintenance of Departmental privacy policies related to the Privacy Act, E- Government Act privacy provisions, Intelligence Reform and Terrorism Prevention Act of 2004, OMB guidance, NIST standards, and related laws, policies and procedures.
- Collaborate with information resource management officials to incorporate privacy requirements and best practices in coordination with bureau senior staff and managers.
- Develop and implement processes and initiatives to assess privacy risk in bureau information systems, websites, programs, projects, information collections, social media, and new technologies.
- Develop and implement strategies and plans for the implementation of privacy protection policy and practices across the bureau throughout the information life cycle in order to meet Federal government compliance requirements and standards for privacy protection in information systems.

Privacy Compliance and Oversight

Oversee and manage bureau privacy program activities including, but not limited to, compliance with the Privacy Act of 1974, the E-Government Act of 2002, Federal Information Security Modernization Act (FISMA), Intelligence Reform and Terrorism Prevention Act of 2004, Health Insurance Portability and Accountability Act (HIPAA), the Electronic Communications Privacy Act, Government Paperwork Elimination Act, Information Protection and Security Act, Identity Theft Prevention Act, Online Privacy Protection and Security Act, Social Security Number Protection Act, OMB Circular A-130 and privacy policies, National Institute of Standards and Technology guidance and standards in coordination with the Departmental Privacy Officer.

- Monitor and analyze privacy laws and requirements, and effectively communicate requirements in writing and orally to other staff.
- Advise and provide guidance to staff to mitigate privacy related risks and ensure compliance with privacy requirements.
- Develop and implement processes and procedures to review proposed data collections in the early stages of the bureau's decision-making process; and ensure the program office has legal authority to collect the information and only collects PII relevant and necessary to support the mission.
- Maintain and regularly update the Bureau's inventory of PII holdings, and work with Bureau officials to minimize the unnecessary collection, use and holdings of Social Security numbers and PII, and report status of PII holdings to the Departmental Privacy Officer in accordance with Federal government mandates and Departmental policy.

- Collaborate with Bureau officials to conduct reviews of PII within the Bureau and with contractors, partners and third parties to ensure ongoing compliance with the Privacy Act and related privacy laws and policies, that appropriate controls are implemented to safeguard PII, memorandums of understanding and agreements are reviewed for adequacy as required to protect privacy, and information sharing activities are conducted in accordance with applicable laws and policies.
- Conduct reviews of prospective contractors or grantees to ensure they can meet privacy requirements, ensure privacy requirements are included in contract, acquisition or grant-related documentation, and audits/reviews for compliance with privacy requirements are conducted regularly during the period of performance.
- Prepare reports to the Office of Management and Budget, Congress, other oversight body and organizations as needed in coordination with the Departmental Privacy Officer, including but not limited to Senior Agency Official for Privacy Reports under FISMA, reports on computer matching, reports on information sharing environment activities as required, etc. to demonstrate accountability and transparency of organizational privacy operations.
- Oversee completion of mandatory annual and role-based privacy training and privacy awareness campaigns efforts by drafting privacy training and awareness plans. Develop privacy awareness communications and deliver targeted role-based training for staff handling PII when needed, and maintain Bureau privacy program information on public websites and Bureau intranet sites as needed to promote employee awareness of privacy requirements and responsibilities.
- Ensure Bureau policies and practices are in compliance with laws, regulatory requirements and Departmental privacy program strategies, procedures and standards.
- Review proposed privacy policies and monitor current policy to ensure implementation and privacy issues are adequately addressed (e.g., Privacy Impact Assessments are completed for Information Technology initiatives).
- Conduct management evaluations and internal control processes to ensure ongoing compliance monitoring of the Bureau privacy program.
- Ensure compliance with privacy practices and take appropriate action to correct deficiencies or failure to comply with privacy policies for the Bureau employee extended workforce, contractors, partners and business associates, in consultation with Human Resources, Bureau leadership, administration, and legal counsel.
- Develop metrics to measure the Bureau's privacy performance, develop strategies for improvement and report findings and recommendations to Bureau management and the Departmental Privacy Officer.
- Provide reports on status of Bureau privacy program activities as required by the Departmental Privacy Officer.

Privacy Analysis and Assessment

Analyzes privacy source systems, databases, projects, and information collections, conducts reviews, and updates privacy compliance documentation in support of the Department in accordance with privacy laws, regulations and policies.

- Maintain Bureau System of Records Notices (SORNs) for records maintained in paper, micro, or electronic format (or a combination of these formats) that contain records about

individuals in accordance with the provisions of the Privacy Act of 1974. Work with system managers to review and update SORNs, and support Departmental Privacy Officer review and approval process for SORN publication in the Federal Register.

- Ensure Privacy Impact Assessments are conducted as required for information systems, projects, information collections developed within the Bureau in accordance with Departmental policy requirements.
- Develop and update privacy notices and Privacy Act Statements for information collections from individuals, and ensure that the purpose for collection is specified in privacy notices, individuals are provided an opportunity to consent to data collection when appropriate, individuals are advised of how to access and correct information about them, and how to contact the Bureau for privacy complaints.
- Prepare responses to questions from employees about handling PII, privacy risks, ways to improve business processes or otherwise mitigate risks, and meet legal and policy requirements.
- Coordinate and implement privacy requirements, policies and procedures, with records management, FOIA, information collection clearance, security and other information management functions.
- Develop and implement processes and procedures to conduct privacy review of proposed new data collections early in the agency's decision-making process, and analyze how PII is handled in current and new technologies, identifying risks utilizing methods and tools used for risk assessment, and advising personnel on ways to mitigate risks.
- Assist in developing and implementing technologies, principles and processes to analyze, prioritize and respond to incidents involving compromise or unauthorized disclosure or access to PII, and regularly review incidents to understand patterns and develop mitigation measures.
- Analyze privacy risks and ensure implementation of privacy controls (including privacy continuous monitoring strategies and controls stated in NIST SP 800-53 Rev. 4, App. J "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 program officials, security, and the Departmental Privacy Officer.

Supervisory

Directs, coordinates, and oversees work of a professional staff. Advises staff regarding policies, procedures, and directives of higher level management. Explains performance expectations and provides regular feedback. Initiates action to correct performance or conduct problems of employees. Reviews developmental needs of staff and encourages self-development. Ensures actions taken promote an environment in which staff members are empowered to participate in and contribute to effective mission accomplishment. Provides a work environment that is free from all forms of discrimination, harassment, and retaliation and supports the agency's EEO program. Addresses staff concerns, whether perceived or real, and follows up with appropriate action to correct or eliminate tension in the workplace. [Additional supervisory responsibilities may be added or edited as appropriate}

Performs other related duties and responsibilities as assigned.

SELECT THE APPROPRIATE GRADE CONTROLLING EVALUATION

SUPERVISORY

Factor 1 – Program Scope and Effect

Level 1-3, 550 Points

The [bureau] is a major bureau/office within the Department of the Interior. The [ORGANIZATIONAL NAME – Office of Information Resources for example] is responsible for [describe mission and responsibilities].

Factor 2 – Organizational Setting

Level 2-2, 250 Points

The incumbent works under the guidance and direction of the bureau Associate Chief Information Officer and in close collaboration with the Departmental Privacy Officer. The incumbent receives direct supervision as well as management support, direction, and oversight from the Associate Chief Information Officer.

Factor 3 – Supervisory and Managerial Authority Exercised Level 3-3b, 775 Points

The employee exercises delegated authority, oversight, and total management of the Bureau Privacy Program consisting of [describe the organizational structure here – how many division and branches] with approximately [number] of employees [if there are multiple layers of management within the organization, please describe].

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

Using 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. Exercising significant responsibilities in dealing with officials of other offices or organizations, or in advising management senior officials. Assuring 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. Making decisions on work problems presented by subordinate supervisors, team leaders, or similar personnel, or by contractors. Evaluating subordinate supervisors or leaders and serving as the reviewing official on evaluations of nonsupervisory employees rated by subordinate supervisors. Making or approving selections for subordinate nonsupervisory positions. Recommending 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. Hearing and resolving group grievances or serious employee complaints.

Factor 4 – Personal Contacts

Subfactor 4A – Nature of Contacts

Level 4A-3, 75 Points

The employee interacts on a daily basis with persons representing organizations or groups from inside and outside the bureau and the Department. This includes senior bureau 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

Level 4B-3, 100 Points

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

Level 5-7, 930 Points

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 the bureau/office leadership and the ACIO and DPO 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, direct operations and studies, and negotiate assignments involves understanding direction and vision of the Departmental Privacy Officer and the bureau, 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-13 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

Level 6-5, 1225 Points

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-13 grade.

Total Points: 3905

GS-14 Point Range: 3605-4050

NONSUPERVISORY

Factor 1. Knowledge Required by the Position: Level 1-8, 1550 Points

Mastery of and skill in applying a wide range of qualitative and quantitative methods for the assessment and improvement of complex privacy related programs, processes and systems, including the sequence and timing of key privacy and security program milestones, and methods to evaluate the worth of the Bureau program accomplishments, as they relate to management of planned privacy program objectives.

Mastery knowledge of a wide range of administrative laws, policies, regulations and precedents including OMB and Department regulations applicable to the administration of the Bureau-wide privacy program sufficient to improve processes, make recommendations to senior management, and provide oversight of the privacy program.

Expert knowledge in the areas of Privacy policy analysis and development, Privacy program development and implementation, information law and disclosure issues, Departmental privacy guidance and compliance programs, employee privacy issues, legislative issues affecting privacy, and various privacy publications sufficient to represent the Bureau.

Comprehensive knowledge of the Privacy Act, OMB guidance, the Computer Matching and Privacy Protection Act, E-Government Act, FISMA, HIPAA, privacy statutory, regulatory and other legal requirements for privacy policy and its application to information resource management, Department policies, and other areas of privacy law in order to meet responsibilities for Bureau compliance initiatives regarding these laws, regulations, and policies.

In-depth knowledge and experience in gathering, assembling, interpreting and analyzing a vast amount of complex privacy and security related technical data and materials, including identifying key issues, drawing sound conclusions and developing authoritative recommendations, approaches and comprehensive management reports concerned with established and/or proposed privacy policies and plans.

Exceptional interpersonal, verbal and written communications skills, sufficient to prepare and present technical material, policy, regulations, guidance, briefing materials, and reports to management in support of the privacy program and in order to brief and guide staff and high level management during privacy breaches, privacy mitigation loss strategies, privacy task force(s) and associated responsibilities.

Demonstrated expert knowledge in conducting Privacy Impact Assessments on highly complex computer and information systems to ensure identification and protection of privacy information.

In-depth knowledge and understanding of the Bureau organizations and various functional operations to develop, implement, and evaluate privacy issues and management and the ability to provide innovative technical direction for resolution of critical problems anticipated in the accomplishment of privacy program requirements.

Expert knowledge of Privacy Act requirements to determine and evaluate the potential effects of privacy requirements on business operations and developing strategies to assist Bureau operations in meeting their privacy and legal policy requirements.

Incumbent must possess high degree of professionalism in demonstrating and applying discretion and judgment when dealing with sensitive issues.

Requires skill in handling criticisms of Bureau performance, to logically and effectively explain issues, programs, functions and activities, providing a better understanding of the organization's efforts to concerned public citizens.

DESIRED: Obtain and maintain at least one of the following privacy professional certifications from the International Association of Privacy Professionals: Certified Information Privacy Professional/US Government (CIPP/G); Certified Information Privacy Manager (CIPM)

Factor 2. Supervisory Controls: Level 2-5, 650 Points

The incumbent works under the general supervision of the Bureau Associate Chief Information Officer and in close collaboration with the Departmental Privacy Officer, with responsibility for meeting Bureau and Departmental level privacy objectives. As a recognized authority and privacy subject matter expert, the incumbent is responsible for the evaluation of privacy program functions and issues, and is subject only to administrative and policy direction concerning overall project priorities and objectives. The incumbent is delegated authority to independently plan, schedule, implement and monitor major projects concerned with the analysis and evaluation of the effectiveness of the Bureau privacy program and privacy initiatives, and communicating pertinent information relative to the Bureau privacy program activities. Analyses, evaluations and recommendations developed by the employee are normally reviewed by management officials only for potential influence on broad agency policy objectives and program goals. Supervision is generally in terms of broad policy and program direction and the incumbent must have the ability to produce and is subject to a high degree on the incumbent's ability to produce and develop high quality actions and recommendations independently. Incumbent initiates and participates in the development of objectives to be accomplished relating to Federal government privacy requirements and privacy protection. The incumbent has wide latitude in establishing priorities, determining approaches and independently planning, designing and carrying out programs, projects, and studies. Determinations, recommendations, and conclusions are considered definitive. Work is reviewed on such matters as fulfillment of program objectives and mission accomplishments.

Factor 3. Guidelines: Level 3-5, 650 Points

Basic guidance may be found in Departmental policy, legislation and regulations that offer very broad operating parameters, including rapidly evolving guidance provided by oversight agencies such as the Office of Management and Budget (OMB), Government Accountability Office, Department of Justice, General Services Administration, and National Institute of Standards and Technology. State, local, and Tribal statutes must be considered as they might

affect or be affected by proposed Federal policies. Incumbent may draft or initiate changes in regulations or Departmental policy for consideration and approval by the DPO. Incumbent must use high levels of originality, judgment, discretion and creativeness to interpret intent and applicability, to adapt to the changing requirements, and to meet customer needs and add value in the most efficient and cost-effective way possible. Guidelines include laws, regulations, Departmental manuals, handbooks, policies, standards, and program documents, other legal requirements of the Federal government and long-range plans. Also included is literature concerning privacy issues and materials dealing with computer technology, organization, management, and evaluation techniques.

The incumbent identifies the need for and develops management and administrative policies, procedures, guidelines, and privacy protection tools needed to ensure compliance with the Privacy Act of 1974, E-Government Act, FISMA, HIPAA, the Intelligence Reform and Terrorism Prevention Act, the Electronic Communications Privacy Act, Government Paperwork Elimination Act, Information Protection and Security Act, Identity Theft Prevention Act, Online Privacy Protection and Security Act, Social Security Number Protection Act, non-disclosure statutes, OMB Circular A-130, OMB policy, NIST standards, Federal Information Processing Standards, specifically FIPS-199, user authentication, and related Federal privacy laws, policy and guidelines.

Factor 4. Complexity: Level 4-5, 325 Points

The incumbent analyzes interrelated issues to determine effectiveness, efficiency, and productivity for Bureau-wide privacy administrative and operational privacy programs. The incumbent develops detailed plans, goals, and end objectives for long-range implementation and administration of the privacy policies, plans and management initiatives. The incumbent develops criteria for evaluating the effectiveness of the privacy program. Decisions concerning planning, organizing and conducting studies are complicated by conflicting laws, program goals and objectives, and the incumbent must ensure that privacy program requirements are met in a way that allows organization mission goals to be completed.

Assignments related to privacy violations may be complicated by the need to deal with subjective concepts, sensitive situations, and combative or defensive parties. Most privacy issues are complex and unique so findings and conclusions may be highly subjective and not readily susceptible to verification through replication of study methods or reevaluation of results. Options, recommendations, and conclusions take into account and give appropriate weight to interpretation of privacy regulations, foreseeable harm to the organization and individuals, severity of events, and a wide range of other variables which affect long-range privacy program performance and direction.

Factor 5. Scope and Effect: Level 5-5, 325 Points

The purpose of the work is to analyze and evaluate privacy implications and protections for major administrative aspects of substantive, mission-oriented programs. This may involve, for example, the development of long-range program plans, goals, objectives, and milestones or evaluating the effectiveness of programs conducted throughout the Bureau. The Bureau's

activities greatly affect the general public and the Bureau's activities are subject to constant controversy and scrutiny from all sources, including the national and local news media, and various interest groups. Privacy is highly visible and compliance with privacy laws and policies is critical to the Bureau's mission. Without appropriate privacy controls in place to safeguard privacy, compromise of government systems and data can have significant impact on individuals, and can affect public confidence and the agency's mission.

Factor 6, Personal Contacts and Factor 7, Purpose of Contacts: Level 3c, 180 Points

Personal Contacts:

Extensive personal contacts are required with executive officials, professional, technical, administrative, and managerial personnel, throughout the Bureau, the Office of the Chief Information Officer, Office of Regulatory Affairs, Office of Policy Analysis and Office of the Solicitor, and staffs at other Bureaus/Offices and at different organizational levels of the Department. Contacts may also be required with the Office of Federal Register, OMB, Federal, state agencies, tribal governments, private industry, and environmental groups. Incumbent has direct liaison with officials from Government-wide committees and working groups, Inter-Governmental organizations, Congressional representatives, law firms, and members of the general public, as well as liaison and collaboration with representatives of stakeholder groups and senior Federal officials.

The incumbent maintains regular contact with interested national and local professional organizations, industry and interest groups, and other non-governmental organizations. Communication with contacts are made through standing coordination meetings, working groups, presentations, personal contact, by telephone, paper or electronic correspondence or any combination of these methods, when such contacts occur on an ad hoc basis.

Purpose of Contacts:

Contacts with the Department, other governmental and non-governmental offices are made to plan, coordinate, advise, secure, direct or influence others regarding significant issues and to resolve problems of mutual concern and ensuring that Privacy Act activities are consistent with legal precedent and policy. The incumbent must represent the Bureau's position on various planning process aspects concerning privacy within and outside the Department. The incumbent proposes solutions and mediates differing objectives into mutually beneficial courses of action to gain acceptance of ideas or to achieve compliance with established privacy policies and regulations.

Contacts with Bureau internal program offices are largely to conduct privacy assessments, evaluate privacy controls and ensure compliance, resolve privacy issues and complaints, perform investigations on incidents, provide privacy program information, training, and guidance, and promote awareness. These contacts also are made to maintain knowledge of current mission objectives, information systems and initiatives, and other program activities as they relate to privacy issues. The incumbent must explain privacy policy positions and make recommendations, and negotiate differences in matters concerning privacy program

responsibilities and mission objectives. The incumbent must frequently present and defend analyses and recommendations in meetings with individuals and organizations with conflicting priorities. The incumbent may negotiate matters and may make commitments within his/her area of responsibility.

Public contacts usually involve coordination 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 8. Physical Demands: Level 8-1, 5 Points

The work is mostly sedentary. Some travel is required, both within and outside the local commuting area. Occasional travel may be required to field activities for compliance review, determination of activity performance, and to conduct training and/or technical assistance. The incumbent must be able to function well under stressful conditions, often working under very tight deadlines involving projects of national significance.

Factor 9. Work Environment: Level 9-1, 5 Points

Work is performed primarily in office areas, conference rooms, and similar environments. No hazardous conditions are anticipated.

TOTAL POINTS = 3690 = GS-14
POINT RANGE = 3605-4050

POSITION DESCRIPTION (Please Read Instructions on the Back)

1. Agency Position No.
DOI1003
 6. OPM Certification No.

2. Reason for Submission
 Redescription New
 Reestablishment Other
 Explanation (Show any positions replaced)

3. Service
 Hdqtrs Field

4. Employing Office Location

5. Duty Station

7. Fair Labor Standards Act
 Exempt Nonexempt

8. Financial Statements Required
 Executive Personnel Financial Disclosure Employment and Financial Interest

9. Subject to IA Action
 Yes No

10. Position Status
 Competitive
 Excepted (Specify in Remarks)
 SES (Gen.) SES (CR)

11. Position Is
 Supervisory Managerial
 Neither

12. Sensitivity
 1--Non-Sensitive 3--Critical
 2--Noncritical Sensitive 4--Special Sensitive

13. Competitive Level Code

14. Agency Use

15. Classified/Graded by	Official Title of Position	Pay Plan	Occupational Code	Grade	Initials	Date
a. Office of Personnel Management						
b. Department, Agency or Establishment						
c. Second Level Review	Government Information Specialist	GS	0306	15		
d. First Level Review						
e. Recommended by Supervisor or Initiating Office						

16. Organizational Title of Position (if different from official title)
Associate Privacy Officer

17. Name of Employee (if vacant, specify)

18. Department, Agency, or Establishment
Department of the Interior

a. First Subdivision

b. Second Subdivision

c. Third Subdivision

d. Fourth Subdivision

e. Fifth Subdivision

19. Employee Review-This is an accurate description of the major duties and responsibilities of my position.

Signature of Employee (optional)

20. **Supervisory Certification.** I certify that this is an accurate statement of the major duties and responsibilities of this position and its organizational relationships, and that the position is necessary to carry out Government functions for which I am responsible. This certification is made with the knowledge that this information is to be used for statutory purposes relating to appointment and payment of public funds, and that false or misleading statements may constitute violations of such statutes or their implementing regulations.

a. Typed Name and Title of Immediate Supervisor

b. Typed Name and Title of Higher-Level Supervisor or Manager (optional)

Signature _____ Date _____


Signature _____ Date _____

21. **Classification/Job Grading Certification.** I certify that this position has been classified/graded as required by Title 5, U.S. Code, in conformance with standards published by the U.S. Office of Personnel Management or, if no published standards apply directly, consistently with the most applicable published standards.

22. Position Classification Standards Used in Classifying/Grading Position

Information for Employees. The standards, and information on their application, are available in the personnel office. The classification of the position may be reviewed and corrected by the agency or the U.S. Office of Personnel Management. Information on classification/job grading appeals, and complaints on exemption from FLSA, is available from the personnel office or the U.S. Office of Personnel Management.

Typed Name and Title of Official Taking Action
Martin Pursley
Director, Talent Management

Signature  Date **10/28/16**

23. Position Review	Initials	Date	Initials	Date	Initials	Date	Initials	Date	Initials	Date
a. Employee (optional)										
b. Supervisor										
- Classifier										
Remarks										

25. Description of Major Duties and Responsibilities (See Attached)

**Department of the Interior
Government Information Specialist
GS-0306-15**

Organizational Title: Associate Privacy Officer

Introduction

This position is for the Department of the Interior (DOI or Department) [bureau/office] Associate Privacy Officer (APO) located in [bureau/office] (bureau). The APO reports directly to the [bureau] Associate Chief Information Officer (ACIO) and is responsible for planning, developing, analyzing, evaluating and administering the Bureau Privacy Program, to include policy and training development, the execution, administration and conduct of the program, oversight of privacy program functions, providing guidance on privacy-related matters, implementing and assessing privacy activities, and establishing plans and strategies for implementing privacy and data protection initiatives. The APO also reports to the Departmental Privacy Officer (DPO) for privacy program compliance activities, and provides collaboration and support for agency privacy program functions. The APO serves as the Bureau privacy subject matter expert and focal point for privacy issues, has Privacy Act oversight and reporting responsibility, and provides guidance and recommendations to Bureau-level senior officials on the implementation of the Department's privacy priorities and plans. The position requires expert technical, research, and analytical skills, to include mastery in interpretation of the Privacy laws and policies. Additionally, incumbent must have superb judgment and have the ability to make sound decisions and provide guidance to top-level Bureau officials.

The primary responsibility of the APO is to provide privacy program advocacy, oversight, leadership and guidance for their Bureau in coordination with the DPO and in alignment with the DOI Privacy Program. The APO must have comprehensive knowledge and understanding of Federal privacy laws and regulatory and policy requirements, and ensures that all Bureau privacy activities adhere to the requirements of the Privacy Act of 1974, the Computer Matching and Privacy Protection Act, the E-Government Act of 2002, the Federal Information Security Modernization Act, the Electronic Communications Privacy Act, the Intelligence Reform and Terrorism Prevention Act of 2004, the Health Insurance Portability and Accountability Act (HIPAA) where applicable, Office of Management and Budget (OMB) directives, National Institute of Standards and Technology (NIST) standards and guidance, DOI Privacy Act and privacy program regulations and policies, and other applicable laws, policies, and standards. The APO ensures privacy laws, regulations and policies are implemented and a privacy framework is established for the protection of information privacy.

Major Duties

Privacy Leadership

The APO is responsible for full Bureau Privacy Program management, leads Bureau Privacy

Program activities and is the primary point of contact with the Departmental Privacy Officer, Federal, Tribal, state and local government offices, organizations, and the public in addressing privacy issues.

- Represent the bureau on activities and requirements of the Privacy Act, privacy provisions of the E-Government Act, Intelligence Reform and Terrorism Prevention Act, and related Federal privacy laws, regulations, and policies.
- Represent bureau interests and participates on intra-Agency, inter-Agency, and inter-governmental committees and task-forces.
- Serve as liaison and subject matter expert on bureau privacy complaints, issues, and problems to assist and advise bureau management, employees, and contractors regarding resolution of problems and privacy-related issues.
- Lead the bureau Identity Theft Task Force and oversee bureau privacy incident response activities to mitigate the impact of privacy incidents on individuals and the agency, provide internal and external notifications as necessary, and ensure appropriate reporting to internal and external organizations in coordination with the Departmental Privacy Officer.
- Develop lessons learned, updates bureau privacy policies and strategies, and provides briefings and reports to bureau leadership and the Departmental Privacy Officer.
- Address bureau privacy program deficiencies with bureau leadership and the Departmental Privacy Officer to improve program functions and maintain compliance with Federal and Departmental privacy requirements.
- Evaluate the effectiveness of bureau privacy policies and practices, and establish plans and strategies to identify ways to mitigate gaps and obtain objectives.
- Develop and provide privacy training, orientation tools and resources for different levels of employees (and contractors) based on roles and responsibilities, as well as specific needs and skill development.
- Provide guidance and prepare responses to privacy questions from bureau officials, and prepare responses to privacy-related inquiries from the Department and other internal and external oversight organizations including Office of Inspector General, Office of Management and Budget, and Congress.
- Initiate appropriate action and oversee privacy complaints in coordination and collaboration with the Department, bureau and program officials, and legal counsel when necessary.
- Coordinate with senior management, legal counsel, and other parties to represent the bureau information privacy interests with internal and external parties on proposed new or amended legislation, regulations, or policies, as well as on audits or reviews of privacy functions or program areas with privacy implications.

Policy Development

The APO oversees the development, implementation, maintenance of, and adherence to bureau policies and procedures covering the collection, handling, safeguarding, sharing and disclosure of personally identifiable information in compliance with Federal laws, Departmental regulations, and privacy policies.

- Develop, update and implement 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.
- Review, analyze and/or develop proposed rulemakings, regulations, guidelines or other documents to determine privacy impacts, communicating those impacts to the appropriate Departmental or bureau officials, working with program officials to revise proposed policy, rulemaking or other documents to address privacy implications and mitigate risks.
- Review and analyze bureau policy or bureau manual chapters, proposed policy guidance, related documents pertaining to Privacy Act systems of records, and any associated rulemaking documentation for effect on bureau mission and program activities.
- Provide guidance and interpretation, and assist in the implementation and maintenance of Departmental privacy policies related to the Privacy Act, E- Government Act privacy provisions, Intelligence Reform and Terrorism Prevention Act of 2004, OMB guidance, NIST standards, and related laws, policies and procedures.
- Collaborate with information resource management officials to incorporate privacy requirements and best practices in coordination with bureau senior staff and managers.
- Develop and implement processes and initiatives to assess privacy risk in bureau information systems, websites, programs, projects, information collections, social media, and new technologies.
- Develop and implement strategies and plans for the implementation of privacy protection policy and practices across the bureau throughout the information life cycle in order to meet Federal government compliance requirements and standards for privacy protection in information systems.

Privacy Compliance and Oversight

Oversee and manage bureau privacy program activities including, but not limited to, compliance with the Privacy Act of 1974, the E-Government Act of 2002, Federal Information Security Modernization Act (FISMA), Intelligence Reform and Terrorism Prevention Act of 2004, Health Insurance Portability and Accountability Act (HIPAA), the Electronic Communications Privacy Act, Government Paperwork Elimination Act, Information Protection and Security Act, Identity Theft Prevention Act, Online Privacy Protection and Security Act, Social Security Number Protection Act, OMB Circular A-130 and privacy policies, National Institute of Standards and Technology guidance and standards in coordination with the Departmental Privacy Officer.

- Monitor and analyze privacy laws and requirements, and effectively communicate requirements in writing and orally to other staff.
- Advise and provide guidance to staff to mitigate privacy related risks and ensure compliance with privacy requirements.
- Develop and implement processes and procedures to review proposed data collections in the early stages of the bureau's decision-making process; and ensure the program office has legal authority to collect the information and only collects PII relevant and necessary to support the mission.
- Maintain and regularly update the Bureau's inventory of PII holdings, and work with Bureau officials to minimize the unnecessary collection, use and holdings of Social Security numbers and PII, and report status of PII holdings to the Departmental Privacy Officer in accordance with Federal government mandates and Departmental policy.

- Collaborate with Bureau officials to conduct reviews of PII within the Bureau and with contractors, partners and third parties to ensure ongoing compliance with the Privacy Act and related privacy laws and policies, that appropriate controls are implemented to safeguard PII, memorandums of understanding and agreements are reviewed for adequacy as required to protect privacy, and information sharing activities are conducted in accordance with applicable laws and policies.
- Conduct reviews of prospective contractors or grantees to ensure they can meet privacy requirements, ensure privacy requirements are included in contract, acquisition or grant-related documentation, and audits/reviews for compliance with privacy requirements are conducted regularly during the period of performance.
- Prepare reports to the Office of Management and Budget, Congress, other oversight body and organizations as needed in coordination with the Departmental Privacy Officer, including but not limited to Senior Agency Official for Privacy Reports under FISMA, reports on computer matching, reports on information sharing environment activities as required, etc. to demonstrate accountability and transparency of organizational privacy operations.
- Oversee completion of mandatory annual and role-based privacy training and privacy awareness campaigns efforts by drafting privacy training and awareness plans. Develop privacy awareness communications and deliver targeted role-based training for staff handling PII when needed, and maintain Bureau privacy program information on public websites and Bureau intranet sites as needed to promote employee awareness of privacy requirements and responsibilities.
- Ensure Bureau policies and practices are in compliance with laws, regulatory requirements and Departmental privacy program strategies, procedures and standards.
- Review proposed privacy policies and monitor current policy to ensure implementation and privacy issues are adequately addressed (e.g., Privacy Impact Assessments are completed for Information Technology initiatives).
- Conduct management evaluations and internal control processes to ensure ongoing compliance monitoring of the Bureau privacy program.
- Ensure compliance with privacy practices and take appropriate action to correct deficiencies or failure to comply with privacy policies for the Bureau employee extended workforce, contractors, partners and business associates, in consultation with Human Resources, Bureau leadership, administration, and legal counsel.
- Develop metrics to measure the Bureau's privacy performance, develop strategies for improvement and report findings and recommendations to Bureau management and the Departmental Privacy Officer.
- Provide reports on status of Bureau privacy program activities as required by the Departmental Privacy Officer.

Privacy Analysis and Assessment

Analyzes privacy source systems, databases, projects, and information collections, conducts reviews, and updates privacy compliance documentation in support of the Department in accordance with privacy laws, regulations and policies.

- Maintain Bureau System of Records Notices (SORNs) for records maintained in paper, micro, or electronic format (or a combination of these formats) that contain records about

individuals in accordance with the provisions of the Privacy Act of 1974. Work with system managers to review and update SORNs, and support Departmental Privacy Officer review and approval process for SORN publication in the Federal Register.

- Ensure Privacy Impact Assessments are conducted as required for information systems, projects, information collections developed within the Bureau in accordance with Departmental policy requirements.
- Develop and update privacy notices and Privacy Act Statements for information collections from individuals, and ensure that the purpose for collection is specified in privacy notices, individuals are provided an opportunity to consent to data collection when appropriate, individuals are advised of how to access and correct information about them, and how to contact the Bureau for privacy complaints.
- Prepare responses to questions from employees about handling PII, privacy risks, ways to improve business processes or otherwise mitigate risks, and meet legal and policy requirements.
- Coordinate and implement privacy requirements, policies and procedures, with records management, FOIA, information collection clearance, security and other information management functions.
- Develop and implement processes and procedures to conduct privacy review of proposed new data collections early in the agency's decision-making process, and analyze how PII is handled in current and new technologies, identifying risks utilizing methods and tools used for risk assessment, and advising personnel on ways to mitigate risks.
- Assist in developing and implementing technologies, principles and processes to analyze, prioritize and respond to incidents involving compromise or unauthorized disclosure or access to PII, and regularly review incidents to understand patterns and develop mitigation measures.
- Analyze privacy risks and ensure implementation of privacy controls (including privacy continuous monitoring strategies and controls stated in NIST SP 800-53 Rev. 4, App. J "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 program officials, security, and the Departmental Privacy Officer.

Performs other related duties and responsibilities as assigned.

Factor Level Descriptions

Factor 1. Knowledge Required by the Position: Level 1-8, 1550 Points

Mastery of and skill in applying a wide range of qualitative and quantitative methods for the assessment and improvement of complex privacy related programs, processes and systems, including the sequence and timing of key privacy and security program milestones, and methods to evaluate the worth of the Bureau program accomplishments, as they relate to management of planned privacy program objectives.

Mastery knowledge of a wide range of administrative laws, policies, regulations and

precedents including OMB and Department regulations applicable to the administration of the Bureau-wide privacy program sufficient to improve processes, make recommendations to senior management, and provide oversight of the privacy program.

Expert knowledge in the areas of Privacy policy analysis and development, Privacy program development and implementation, information law and disclosure issues, Departmental privacy guidance and compliance programs, employee privacy issues, legislative issues affecting privacy, and various privacy publications sufficient to represent the Bureau.

Comprehensive knowledge of the Privacy Act, OMB guidance, the Computer Matching and Privacy Protection Act, E-Government Act, FISMA, HIPAA, privacy statutory, regulatory and other legal requirements for privacy policy and its application to information resource management, Department policies, and other areas of privacy law in order to meet responsibilities for Bureau compliance initiatives regarding these laws, regulations, and policies.

In-depth knowledge and experience in gathering, assembling, interpreting and analyzing a vast amount of complex privacy and security related technical data and materials, including identifying key issues, drawing sound conclusions and developing authoritative recommendations, approaches and comprehensive management reports concerned with established and/or proposed privacy policies and plans.

Exceptional interpersonal, verbal and written communications skills, sufficient to prepare and present technical material, policy, regulations, guidance, briefing materials, and reports to management in support of the privacy program and in order to brief and guide staff and high level management during privacy breaches, privacy mitigation loss strategies, privacy task force(s) and associated responsibilities.

Demonstrated expert knowledge in conducting Privacy Impact Assessments on highly complex computer and information systems to ensure identification and protection of privacy information.

In-depth knowledge and understanding of the Bureau organizations and various functional operations to develop, implement, and evaluate privacy issues and management and the ability to provide innovative technical direction for resolution of critical problems anticipated in the accomplishment of privacy program requirements.

Expert knowledge of Privacy Act requirements to determine and evaluate the potential effects of privacy requirements on business operations and developing strategies to assist Bureau operations in meeting their privacy and legal policy requirements.

Incumbent must possess high degree of professionalism in demonstrating and applying discretion and judgment when dealing with sensitive issues.

Requires skill in handling criticisms of Bureau performance, to logically and effectively explain issues, programs, functions and activities, providing a better understanding of the organization's

efforts to concerned public citizens.

DESIRED: Obtain and maintain at least one of the following privacy professional certifications from the International Association of Privacy Professionals: Certified Information Privacy Professional/US Government (CIPP/G); Certified Information Privacy Manager (CIPM)

Factor 2. Supervisory Controls: Level 2-5, 650 Points

The incumbent works under the general supervision of the Bureau Associate Chief Information Officer and in close collaboration with the Departmental Privacy Officer, with responsibility for meeting Bureau and Departmental level privacy objectives. As a recognized authority and privacy subject matter expert, the incumbent is responsible for the evaluation of privacy program functions and issues, and is subject only to administrative and policy direction concerning overall project priorities and objectives. The incumbent is delegated authority to independently plan, schedule, implement and monitor major projects concerned with the analysis and evaluation of the effectiveness of the Bureau privacy program and privacy initiatives, and communicating pertinent information relative to the Bureau privacy program activities. Analyses, evaluations and recommendations developed by the employee are normally reviewed by management officials only for potential influence on broad agency policy objectives and program goals. Supervision is generally in terms of broad policy and program direction and the incumbent must have the ability to produce and is subject to a high degree on the incumbent's ability to produce and develop high quality actions and recommendations independently. Incumbent initiates and participates in the development of objectives to be accomplished relating to Federal government privacy requirements and privacy protection. The incumbent has wide latitude in establishing priorities, determining approaches and independently planning, designing and carrying out programs, projects, and studies. Determinations, recommendations, and conclusions are considered definitive. Work is reviewed on such matters as fulfillment of program objectives and mission accomplishments.

Factor 3. Guidelines: Level 3-5, 650 Points

Basic guidance may be found in Departmental policy, legislation and regulations that offer very broad operating parameters, including rapidly evolving guidance provided by oversight agencies such as the Office of Management and Budget (OMB), Government Accountability Office, Department of Justice, General Services Administration, and National Institute of Standards and Technology. State, local, and Tribal statutes must be considered as they might affect or be affected by proposed Federal policies. Incumbent may draft or initiate changes in regulations or Departmental policy for consideration and approval by the DPO. Incumbent must use high levels of originality, judgment, discretion and creativeness to interpret intent and applicability, to adapt to the changing requirements, and to meet customer needs and add value in the most efficient and cost-effective way possible. Guidelines include laws, regulations, Departmental manuals, handbooks, policies, standards, and program documents, other legal requirements of the Federal government and long-range plans. Also included is literature concerning privacy issues and materials dealing with computer technology, organization, management, and evaluation techniques.

The incumbent identifies the need for and develops management and administrative policies, procedures, guidelines, and privacy protection tools needed to ensure compliance with the Privacy Act of 1974, E-Government Act, FISMA, HIPAA, the Intelligence Reform and Terrorism Prevention Act, the Electronic Communications Privacy Act, Government Paperwork Elimination Act, Information Protection and Security Act, Identity Theft Prevention Act, Online Privacy Protection and Security Act, Social Security Number Protection Act, non-disclosure statutes, OMB Circular A-130, OMB policy, NIST standards, Federal Information Processing Standards, specifically FIPS-199, user authentication, and related Federal privacy laws, policy and guidelines.

Factor 4. Complexity: Level 4-6, 450 Points

The work is highly technical in nature, covering a full range of program and administrative management problems and requiring a thorough knowledge and background in privacy issues as they relate to paper and electronic records. Novel and unprecedented situations arise with high frequency, requiring extensive research and analysis to determine the nature of the problem and to identify and negotiate resolutions. Typical assignments include simultaneous actions within and outside the organization, agency, and sometimes government.

Assignments are characterized by a requirement for a broad viewpoint and involve several phases, which must be interrelated and coordinated. Factors to be considered involve major areas of uncertainty in approach, methodology and technical considerations. Difficulty is encountered in separating the substantive nature of the programs or issues studied to the administrative, technical, political, economic, fiscal and other components, and determining how to translate the intent into program actions. Because of the critical nature of the issues evaluated, extensive collaboration and support of experts in other areas is required. Many initiatives are interagency in nature and require an additional level of coordination.

Duties not only require involvement in strategic and tactical planning, but also include the responsibilities for quality control and ensuring that programs are in place and in compliance with department program quality standards. The work requires analysis of voluminous amounts of complex material for the purpose of managing the program and resolving problems and concerns that arise. Projects usually involve structure and reporting relationships that depart from past approaches and traditional techniques. Very little guidance is available, requiring the incumbent to carry out these duties in a highly original and collaborative fashion, often involving several groups and teams, as well as a variety of other internal and external customers/stakeholders.

Factor 5. Scope and Effect: Level 5-6, 450 Points

The purpose of the work is to address day-to-day privacy and other management issues and to generate solutions to critical problems by developing methods, tools, and strategies. Recommendations made may result in policy or procedural changes or revised program emphasis on bureau-wide privacy policies, guidelines, and procedures. The responsibilities of the incumbent are critical to compliance with Government privacy protection requirements

related to information systems, websites, new technology, and paper file systems. They are also critical in ensuring that bureau and Departmental interests are addressed in intra- and inter-governmental privacy interests. Assignments are of major importance to each of several departments and agencies. Studies frequently involve extensive problems of coordination in fact-finding and in reviewing and testing recommendation in interested agencies or with outside groups.

Failure to manage privacy issues could and has made the bureau and the Department vulnerable to civil and criminal penalties, and censure by Congress and privacy advocate groups. Appropriate privacy protections relating to E-Government initiatives are essential for success of these projects to secure public and employee confidence in use of E-Government solutions. Noncompliance with OMB and statutory requirements can jeopardize the bureau's and the Department's ability to meet its fiduciary responsibilities or obtain funding for major projects if budget submissions do not meet OMB standards. This will adversely impact the ability of the bureau and the Department to accomplish its mission.

The bureau's activities are subject to constant controversy and scrutiny from all sources, including the national and local new media, and various interest groups (such as non-Government Privacy Advocacy groups). Privacy concerns in IT programs are highly visible and involve sensitive components of the bureau's and the Department's missions.

Factor 6, Personal Contacts and Factor 7, Purpose of Contacts: Level 4D, 330 Points

Personal Contacts:

Extensive personal contacts are required with executive officials and staffs at all organizational levels of the bureau and the Department. Incumbent has direct liaison with officials at OMB, Government-wide committees, intergovernmental organization as well as liaison and collaboration with stakeholder groups and senior federal official. The incumbent maintains regular contact with interested national and local professional organizations, industry and interest groups, and other non-governmental organizations. Other contacts vary widely and include all levels of the Department, counterparts in other Federal, state and Tribal organizations, private sector officials, Congressional representatives, law firms, and members of the general public. Contacts may be in person, by telephone, paper or electronic correspondence or any combination of these methods.

Contacts are made to plan, coordinate, advise, secure, direct or influence others against significant issues and to resolve problems and mutual concern. The incumbent must represent and defend the bureau's position on various planning process aspects concerning privacy within and outside the bureau. The incumbent proposes solutions and mediates differing objectives into mutually beneficial courses of action to gain acceptance of ideas or to achieve compliance with established policies and regulations.

Contacts serve to justify or settle matters involving significant or controversial issues, coordinate work, discuss issues, exchange information, resolve problems, explain policy positions, make recommendations, and negotiate differences in matters concerning the other

areas of program responsibility. The incumbent must frequently present and defend analyses and recommendations in meetings with individuals and organizations with conflicting priorities. The incumbent may negotiate matters and may make commitments within his/her area of responsibility.

Contacts with the Department and other bureaus are largely to resolve issues, acquire input from customers, and obtain or provide needed information. Personal contacts also are to maintain knowledge or current techniques in the natural resources management, IT and associate professions as they relate to records issues. Public contacts usually involve coordination and information gathering, as well as explaining department programs and policies or facilitating the building of consensus positions on issues from several divergent and conflicting advocates or groups.


Factor 8. Physical Demands: Level 8-1, 5 Points

The work is mostly sedentary. Some travel is required, both within and outside the local commuting area. Occasional travel may be required to field activities for compliance review, determination of activity performance, and to conduct training and/or technical assistance. The incumbent must be able to function well under stressful conditions, often working under very tight deadlines involving projects of national significance.

Factor 9. Work Environment: Level 9-1, 5 Points

Work is performed primarily in office areas, conference rooms, and similar environments. No hazardous conditions are anticipated.

TOTAL POINTS = 4090 = GS-15
POINT RANGE = 4055 and above

POSITION DESCRIPTION <i>(Please Read Instructions on the Back)</i>						1. Agency Position No. DOI1004							
2. Reason for Submission <input type="checkbox"/> Redescription <input checked="" type="checkbox"/> New <input type="checkbox"/> Reestablishment <input type="checkbox"/> Other <small>Explanation (Show any positions replaced)</small>		3. Service <input checked="" type="checkbox"/> Hdqtrs <input type="checkbox"/> Field		4. Employing Office Location		5. Duty Station		6. OPM Certification No.					
		7. Fair Labor Standards Act <input checked="" type="checkbox"/> Exempt <input type="checkbox"/> Nonexempt		8. Financial Statements Required <input type="checkbox"/> Executive Personnel Financial Disclosure <input type="checkbox"/> Employment and Financial Interest		9. Subject to IA Action <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No		13. Competitive Level Code					
		10. Position Status <input type="checkbox"/> Competitive <input type="checkbox"/> Excepted <i>(Specify in Remarks)</i> <input type="checkbox"/> SES (Gen.) <input type="checkbox"/> SES (CR)		11. Position Is <input checked="" type="checkbox"/> Supervisory <input type="checkbox"/> Managerial <input type="checkbox"/> Neither		12. Sensitivity <input type="checkbox"/> 1--Non-Sensitive <input type="checkbox"/> 3--Critical <input type="checkbox"/> 2--Noncritical Sensitive <input type="checkbox"/> 4--Special Sensitive		14. Agency Use					
15. Classified/Graded by		Official Title of Position		Pay Plan		Occupational Code		Grade		Initials		Date	
a. Office of Personnel Management													
b. Department, Agency or Establishment													
c. Second Level Review		Supervisory Government Information Specialist		GS		0306		15					
d. First Level Review													
e. Recommended by Supervisor or Initiating Office													
16. Organizational Title of Position <i>(if different from official title)</i> Associate Privacy Officer						17. Name of Employee <i>(if vacant, specify)</i>							
18. Department, Agency, or Establishment Department of the Interior						c. Third Subdivision							
a. First Subdivision						d. Fourth Subdivision							
b. Second Subdivision						e. Fifth Subdivision							
19. Employee Review-This is an accurate description of the major duties and responsibilities of my position.						Signature of Employee <i>(optional)</i>							
20. Supervisory Certification. <i>I certify that this is an accurate statement of the major duties and responsibilities of this position and its organizational relationships, and that the position is necessary to carry out Government functions for which I am responsible. This certification is made with the knowledge that</i>						<i>this information is to be used for statutory purposes relating to appointment and payment of public funds, and that false or misleading statements may constitute violations of such statutes or their implementing regulations.</i>							
a. Typed Name and Title of Immediate Supervisor						b. Typed Name and Title of Higher-Level Supervisor or Manager <i>(optional)</i>							
Signature						Signature							
Date						Date							
21. Classification/Job Grading Certification. <i>I certify that this position has been classified/graded as required by Title 5, U.S. Code, in conformance with standards published by the U.S. Office of Personnel Management or, if no published standards apply directly, consistently with the most applicable published standards.</i>						22. Position Classification Standards Used in Classifying/Grading Position							
Typed Name and Title of Official Taking Action Martin Pursley Director, Talent Management						Information for Employees. The standards, and information on their application, are available in the personnel office. The classification of the position may be reviewed and corrected by the agency or the U.S. Office of Personnel Management. Information on classification/job grading appeals, and complaints on exemption from FLSA, is available from the personnel office or the U.S. Office of Personnel Management.							
Signature 													
Date 10/28/16													
23. Position Review		Initials		Date		Initials		Date		Initials		Date	
a. Employee <i>(optional)</i>													
b. Supervisor													
Classifier													
Remarks													
25. Description of Major Duties and Responsibilities <i>(See Attached)</i>													

Department of the Interior
Supervisory Government Information Specialist
GS-0306-15

Organizational Title: Associate Privacy Officer

Introduction

This position is for the Department of the Interior (DOI or Department) [bureau/office] Associate Privacy Officer (APO) located in [bureau/office] (bureau). The APO reports directly to the [bureau] Associate Chief Information Officer (ACIO) and is responsible for planning, developing, analyzing, evaluating and administering the Bureau Privacy Program, to include policy and training development, the execution, administration and conduct of the program, oversight of privacy program functions, providing guidance on privacy-related matters, implementing and assessing privacy activities, and establishing plans and strategies for implementing privacy and data protection initiatives. The APO also reports to the Departmental Privacy Officer (DPO) for privacy program compliance activities, and provides collaboration and support for agency privacy program functions. The APO serves as the Bureau privacy subject matter expert and focal point for privacy issues, has Privacy Act oversight and reporting responsibility, and provides guidance and recommendations to Bureau-level senior officials on the implementation of the Department's privacy priorities and plans. The position requires expert technical, research, and analytical skills, to include mastery in interpretation of the Privacy laws and policies. Additionally, incumbent must have superb judgment and have the ability to make sound decisions and provide guidance to top-level Bureau officials.

The primary responsibility of the APO is to provide privacy program advocacy, oversight, leadership and guidance for their Bureau in coordination with the DPO and in alignment with the DOI Privacy Program. The APO must have comprehensive knowledge and understanding of Federal privacy laws and regulatory and policy requirements, and ensures that all Bureau privacy activities adhere to the requirements of the Privacy Act of 1974, the Computer Matching and Privacy Protection Act, the E-Government Act of 2002, the Federal Information Security Modernization Act, the Electronic Communications Privacy Act, the Intelligence Reform and Terrorism Prevention Act of 2004, the Health Insurance Portability and Accountability Act (HIPAA) where applicable, Office of Management and Budget (OMB) directives, National Institute of Standards and Technology (NIST) standards and guidance, DOI Privacy Act and privacy program regulations and policies, and other applicable laws, policies, and standards. The APO ensures privacy laws, regulations and policies are implemented and a privacy framework is established for the protection of information privacy.

Major Duties

Privacy Leadership

The APO is responsible for full Bureau Privacy Program management, leads Bureau Privacy Program activities and is the primary point of contact with the Departmental Privacy Officer,

Federal, Tribal, state and local government offices, organizations, and the public in addressing privacy issues.

- Represent the bureau on activities and requirements of the Privacy Act, privacy provisions of the E-Government Act, Intelligence Reform and Terrorism Prevention Act, and related Federal privacy laws, regulations, and policies.
- Represent bureau interests and participates on intra-Agency, inter-Agency, and inter-governmental committees and task-forces.
- Serve as liaison and subject matter expert on bureau privacy complaints, issues, and problems to assist and advise bureau management, employees, and contractors regarding resolution of problems and privacy-related issues.
- Lead the bureau Identity Theft Task Force and oversee bureau privacy incident response activities to mitigate the impact of privacy incidents on individuals and the agency, provide internal and external notifications as necessary, and ensure appropriate reporting to internal and external organizations in coordination with the Departmental Privacy Officer.
- Develop lessons learned, updates bureau privacy policies and strategies, and provides briefings and reports to bureau leadership and the Departmental Privacy Officer.
- Address bureau privacy program deficiencies with bureau leadership and the Departmental Privacy Officer to improve program functions and maintain compliance with Federal and Departmental privacy requirements.
- Evaluate the effectiveness of bureau privacy policies and practices, and establish plans and strategies to identify ways to mitigate gaps and obtain objectives.
- Develop and provide privacy training, orientation tools and resources for different levels of employees (and contractors) based on roles and responsibilities, as well as specific needs and skill development.
- Provide guidance and prepare responses to privacy questions from bureau officials, and prepare responses to privacy-related inquiries from the Department and other internal and external oversight organizations including Office of Inspector General, Office of Management and Budget, and Congress.
- Initiate appropriate action and oversee privacy complaints in coordination and collaboration with the Department, bureau and program officials, and legal counsel when necessary.
- Coordinate with senior management, legal counsel, and other parties to represent the bureau information privacy interests with internal and external parties on proposed new or amended legislation, regulations, or policies, as well as on audits or reviews of privacy functions or program areas with privacy implications.

Policy Development

The APO oversees the development, implementation, maintenance of, and adherence to bureau policies and procedures covering the collection, handling, safeguarding, sharing and disclosure of personally identifiable information in compliance with Federal laws, Departmental regulations, and privacy policies.

- Develop, update and implement 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.

- Review, analyze and/or develop proposed rulemakings, regulations, guidelines or other documents to determine privacy impacts, communicating those impacts to the appropriate Departmental or bureau officials, working with program officials to revise proposed policy, rulemaking or other documents to address privacy implications and mitigate risks.
- Review and analyze bureau policy or bureau manual chapters, proposed policy guidance, related documents pertaining to Privacy Act systems of records, and any associated rulemaking documentation for effect on bureau mission and program activities.
- Provide guidance and interpretation, and assist in the implementation and maintenance of Departmental privacy policies related to the Privacy Act, E- Government Act privacy provisions, Intelligence Reform and Terrorism Prevention Act of 2004, OMB guidance, NIST standards, and related laws, policies and procedures.
- Collaborate with information resource management officials to incorporate privacy requirements and best practices in coordination with bureau senior staff and managers.
- Develop and implement processes and initiatives to assess privacy risk in bureau information systems, websites, programs, projects, information collections, social media, and new technologies.
- Develop and implement strategies and plans for the implementation of privacy protection policy and practices across the bureau throughout the information life cycle in order to meet Federal government compliance requirements and standards for privacy protection in information systems.

Privacy Compliance and Oversight

Oversee and manage bureau privacy program activities including, but not limited to, compliance with the Privacy Act of 1974, the E-Government Act of 2002, Federal Information Security Modernization Act (FISMA), Intelligence Reform and Terrorism Prevention Act of 2004, Health Insurance Portability and Accountability Act (HIPAA), the Electronic Communications Privacy Act, Government Paperwork Elimination Act, Information Protection and Security Act, Identity Theft Prevention Act, Online Privacy Protection and Security Act, Social Security Number Protection Act, OMB Circular A-130 and privacy policies, National Institute of Standards and Technology guidance and standards in coordination with the Departmental Privacy Officer.

- Monitor and analyze privacy laws and requirements, and effectively communicate requirements in writing and orally to other staff.
- Advise and provide guidance to staff to mitigate privacy related risks and ensure compliance with privacy requirements.
- Develop and implement processes and procedures to review proposed data collections in the early stages of the bureau's decision-making process; and ensure the program office has legal authority to collect the information and only collects PII relevant and necessary to support the mission.
- Maintain and regularly update the Bureau's inventory of PII holdings, and work with Bureau officials to minimize the unnecessary collection, use and holdings of Social Security numbers and PII, and report status of PII holdings to the Departmental Privacy Officer in accordance with Federal government mandates and Departmental policy.
- Collaborate with Bureau officials to conduct reviews of PII within the Bureau and with

contractors, partners and third parties to ensure ongoing compliance with the Privacy Act and related privacy laws and policies, that appropriate controls are implemented to safeguard PII, memorandums of understanding and agreements are reviewed for adequacy as required to protect privacy, and information sharing activities are conducted in accordance with applicable laws and policies.

- Conduct reviews of prospective contractors or grantees to ensure they can meet privacy requirements, ensure privacy requirements are included in contract, acquisition or grant-related documentation, and audits/reviews for compliance with privacy requirements are conducted regularly during the period of performance.
- Prepare reports to the Office of Management and Budget, Congress, other oversight body and organizations as needed in coordination with the Departmental Privacy Officer, including but not limited to Senior Agency Official for Privacy Reports under FISMA, reports on computer matching, reports on information sharing environment activities as required, etc. to demonstrate accountability and transparency of organizational privacy operations.
- Oversee completion of mandatory annual and role-based privacy training and privacy awareness campaigns efforts by drafting privacy training and awareness plans. Develop privacy awareness communications and deliver targeted role-based training for staff handling PII when needed, and maintain Bureau privacy program information on public websites and Bureau intranet sites as needed to promote employee awareness of privacy requirements and responsibilities.
- Ensure Bureau policies and practices are in compliance with laws, regulatory requirements and Departmental privacy program strategies, procedures and standards.
- Review proposed privacy policies and monitor current policy to ensure implementation and privacy issues are adequately addressed (e.g., Privacy Impact Assessments are completed for Information Technology initiatives).
- Conduct management evaluations and internal control processes to ensure ongoing compliance monitoring of the Bureau privacy program.
- Ensure compliance with privacy practices and take appropriate action to correct deficiencies or failure to comply with privacy policies for the Bureau employee extended workforce, contractors, partners and business associates, in consultation with Human Resources, Bureau leadership, administration, and legal counsel.
- Develop metrics to measure the Bureau's privacy performance, develop strategies for improvement and report findings and recommendations to Bureau management and the Departmental Privacy Officer.
- Provide reports on status of Bureau privacy program activities as required by the Departmental Privacy Officer.

Privacy Analysis and Assessment

Analyzes privacy source systems, databases, projects, and information collections, conducts reviews, and updates privacy compliance documentation in support of the Department in accordance with privacy laws, regulations and policies.

- Maintain Bureau System of Records Notices (SORNs) for records maintained in paper, micro, or electronic format (or a combination of these formats) that contain records about individuals in accordance with the provisions of the Privacy Act of 1974. Work with

system managers to review and update SORNs, and support Departmental Privacy Officer review and approval process for SORN publication in the Federal Register.

- Ensure Privacy Impact Assessments are conducted as required for information systems, projects, information collections developed within the Bureau in accordance with Departmental policy requirements.
- Develop and update privacy notices and Privacy Act Statements for information collections from individuals, and ensure that the purpose for collection is specified in privacy notices, individuals are provided an opportunity to consent to data collection when appropriate, individuals are advised of how to access and correct information about them, and how to contact the Bureau for privacy complaints.
- Prepare responses to questions from employees about handling PII, privacy risks, ways to improve business processes or otherwise mitigate risks, and meet legal and policy requirements.
- Coordinate and implement privacy requirements, policies and procedures, with records management, FOIA, information collection clearance, security and other information management functions.
- Develop and implement processes and procedures to conduct privacy review of proposed new data collections early in the agency's decision-making process, and analyze how PII is handled in current and new technologies, identifying risks utilizing methods and tools used for risk assessment, and advising personnel on ways to mitigate risks.
- Assist in developing and implementing technologies, principles and processes to analyze, prioritize and respond to incidents involving compromise or unauthorized disclosure or access to PII, and regularly review incidents to understand patterns and develop mitigation measures.
- Analyze privacy risks and ensure implementation of privacy controls (including privacy continuous monitoring strategies and controls stated in NIST SP 800-53 Rev. 4, App. J "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 program officials, security, and the Departmental Privacy Officer.

Supervisory

Directs, coordinates, and oversees work of a professional staff. Advises staff regarding policies, procedures, and directives of higher level management. Explains performance expectations and provides regular feedback. Initiates action to correct performance or conduct problems of employees. Reviews developmental needs of staff and encourages self-development. Ensures actions taken promote an environment in which staff members are empowered to participate in and contribute to effective mission accomplishment. Provides a work environment that is free from all forms of discrimination, harassment, and retaliation and supports the agency's EEO program. Addresses staff concerns, whether perceived or real, and follows up with appropriate action to correct or eliminate tension in the workplace. [Additional supervisory responsibilities may be added or edited as appropriate]

Performs other related duties and responsibilities as assigned.

SELECT THE APPROPRIATE GRADE CONTROLLING EVALUATION

SUPERVISORY

Factor 1 – Program Scope and Effect

Level 1-3, 550 Points

The [bureau] is a major bureau/office within the Department of the Interior. The [ORGANIZATIONAL NAME – Office of Information Resources for example] is responsible for [describe mission and responsibilities].

Factor 2 – Organizational Setting

Level 2-2, 250 Points

The incumbent works under the guidance and direction of the bureau Associate Chief Information Officer and in close collaboration with the Departmental Privacy Officer. The incumbent receives direct supervision as well as management support, direction, and oversight from the Associate Chief Information Officer.

Factor 3 – Supervisory and Managerial Authority Exercised **Level 3-3b, 775 Points**

The employee exercises delegated authority, oversight, and total management of the Bureau Privacy program consisting of [describe the organizational structure here – how many division and branches] with approximately [number] of employees [if there are multiple layers of management within the organization, please describe].

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

Using 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. Exercising significant responsibilities in dealing with officials of other offices or organizations, or in advising management senior officials. Assuring 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. Making decisions on work problems presented by subordinate supervisors, team leaders, or similar personnel, or by contractors. Evaluating subordinate supervisors or leaders and serving as the reviewing official on evaluations of nonsupervisory employees rated by subordinate supervisors. Making or approving selections for subordinate nonsupervisory positions. Recommending 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. Hearing and resolving group grievances or serious employee complaints.

Factor 4 – Personal Contacts

Subfactor 4A – Nature of Contacts

Level 4A-3, 75 Points

The employee interacts on a daily basis with persons representing organizations or groups from inside and outside the bureau and the Department. This includes senior bureau 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

Level 4B-3, 100 Points

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

Level 5-8, 1030 Points

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 the bureau/office leadership and the ACIO and DPO 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, direct operations and studies, and negotiate assignments involves understanding direction and vision of the Departmental Privacy Officer and the bureau, 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

Level 6-6, 1325 Points

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.

Total Points: 4105

GS-14 Point Range: 4055 and up

NON SUPERVISORY

Factor 1. Knowledge Required by the Position: Level 1-8, 1550 Points

Mastery of and skill in applying a wide range of qualitative and quantitative methods for the assessment and improvement of complex privacy related programs, processes and systems, including the sequence and timing of key privacy and security program milestones, and methods to evaluate the worth of the Bureau program accomplishments, as they relate to management of planned privacy program objectives.

Mastery knowledge of a wide range of administrative laws, policies, regulations and precedents including OMB and Department regulations applicable to the administration of the Bureau-wide privacy program sufficient to improve processes, make recommendations to senior management, and provide oversight of the privacy program.

Expert knowledge in the areas of Privacy policy analysis and development, Privacy program development and implementation, information law and disclosure issues, Departmental privacy guidance and compliance programs, employee privacy issues, legislative issues affecting privacy, and various privacy publications sufficient to represent the Bureau.

Comprehensive knowledge of the Privacy Act, OMB guidance, the Computer Matching and Privacy Protection Act, E-Government Act, FISMA, HIPAA, privacy statutory, regulatory and other legal requirements for privacy policy and its application to information resource management, Department policies, and other areas of privacy law in order to meet responsibilities for Bureau compliance initiatives regarding these laws, regulations, and policies.

In-depth knowledge and experience in gathering, assembling, interpreting and analyzing a vast amount of complex privacy and security related technical data and materials, including identifying key issues, drawing sound conclusions and developing authoritative recommendations, approaches and comprehensive management reports concerned with established and/or proposed privacy policies and plans.

Exceptional interpersonal, verbal and written communications skills, sufficient to prepare and present technical material, policy, regulations, guidance, briefing materials, and reports to management in support of the privacy program and in order to brief and guide staff and high level management during privacy breaches, privacy mitigation loss strategies, privacy task force(s) and associated responsibilities.

Demonstrated expert knowledge in conducting Privacy Impact Assessments on highly complex computer and information systems to ensure identification and protection of privacy information.

In-depth knowledge and understanding of the Bureau organizations and various functional operations to develop, implement, and evaluate privacy issues and management and the ability to provide innovative technical direction for resolution of critical problems anticipated in the accomplishment of privacy program requirements.

Expert knowledge of Privacy Act requirements to determine and evaluate the potential effects of privacy requirements on business operations and developing strategies to assist Bureau operations in meeting their privacy and legal policy requirements.

Incumbent must possess high degree of professionalism in demonstrating and applying discretion and judgment when dealing with sensitive issues.

Requires skill in handling criticisms of Bureau performance, to logically and effectively explain issues, programs, functions and activities, providing a better understanding of the organization's efforts to concerned public citizens.

DESIRED: Obtain and maintain at least one of the following privacy professional certifications from the International Association of Privacy Professionals: Certified Information Privacy Professional/US Government (CIPP/G); Certified Information Privacy Manager (CIPM)

Factor 2. Supervisory Controls: Level 2-5, 650 Points

The incumbent works under the general supervision of the Bureau Associate Chief Information Officer and in close collaboration with the Departmental Privacy Officer, with responsibility for meeting Bureau and Departmental level privacy objectives. As a recognized authority and privacy subject matter expert, the incumbent is responsible for the evaluation of privacy program functions and issues, and is subject only to administrative and policy direction concerning overall project priorities and objectives. The incumbent is delegated authority to independently plan, schedule, implement and monitor major projects concerned with the analysis and evaluation of the effectiveness of the Bureau privacy program and privacy initiatives, and communicating pertinent information relative to the Bureau privacy program activities. Analyses, evaluations and recommendations developed by the employee are normally reviewed by management officials only for potential influence on broad agency policy objectives and program goals. Supervision is generally in terms of broad policy and program direction and the incumbent must have the ability to produce and is subject to a high degree on the incumbent's ability to produce and develop high quality actions and recommendations independently. Incumbent initiates and participates in the development of objectives to be accomplished relating to Federal government privacy requirements and privacy protection. The incumbent has wide latitude in establishing priorities, determining approaches and independently planning, designing and carrying out programs, projects, and studies. Determinations, recommendations, and conclusions are considered definitive. Work is reviewed on such matters as fulfillment of program objectives and mission accomplishments.

Factor 3. Guidelines: Level 3-5, 650 Points

Basic guidance may be found in Departmental policy, legislation and regulations that offer very broad operating parameters, including rapidly evolving guidance provided by oversight agencies such as the Office of Management and Budget (OMB), Government Accountability Office, Department of Justice, General Services Administration, and National Institute of Standards and Technology. State, local, and Tribal statutes must be considered as they might

affect or be affected by proposed Federal policies. Incumbent may draft or initiate changes in regulations or Departmental policy for consideration and approval by the DPO. Incumbent must use high levels of originality, judgment, discretion and creativeness to interpret intent and applicability, to adapt to the changing requirements, and to meet customer needs and add value in the most efficient and cost-effective way possible. Guidelines include laws, regulations, Departmental manuals, handbooks, policies, standards, and program documents, other legal requirements of the Federal government and long-range plans. Also included is literature concerning privacy issues and materials dealing with computer technology, organization, management, and evaluation techniques.

The incumbent identifies the need for and develops management and administrative policies, procedures, guidelines, and privacy protection tools needed to ensure compliance with the Privacy Act of 1974, E-Government Act, FISMA, HIPAA, the Intelligence Reform and Terrorism Prevention Act, the Electronic Communications Privacy Act, Government Paperwork Elimination Act, Information Protection and Security Act, Identity Theft Prevention Act, Online Privacy Protection and Security Act, Social Security Number Protection Act, non-disclosure statutes, OMB Circular A-130, OMB policy, NIST standards, Federal Information Processing Standards, specifically FIPS-199, user authentication, and related Federal privacy laws, policy and guidelines.

Factor 4. Complexity: Level 4-6, 450 Points

The work is highly technical in nature, covering a full range of program and administrative management problems and requiring a thorough knowledge and background in privacy issues as they relate to paper and electronic records. Novel and unprecedented situations arise with high frequency, requiring extensive research and analysis to determine the nature of the problem and to identify and negotiate resolutions. Typical assignments include simultaneous actions within and outside the organization, agency, and sometimes government.

Assignments are characterized by a requirement for a broad viewpoint and involve several phases, which must be interrelated and coordinated. Factors to be considered involve major areas of uncertainty in approach, methodology and technical considerations. Difficulty is encountered in separating the substantive nature of the programs or issues studied to the administrative, technical, political, economic, fiscal and other components, and determining how to translate the intent into program actions. Because of the critical nature of the issues evaluated, extensive collaboration and support of experts in other areas is required. Many initiatives are interagency in nature and require an additional level of coordination.

Duties not only require involvement in strategic and tactical planning, but also include the responsibilities for quality control and ensuring that programs are in place and in compliance with department program quality standards. The work requires analysis of voluminous amounts of complex material for the purpose of managing the program and resolving problems and concerns that arise. Projects usually involve structure and reporting relationships that depart from past approaches and traditional techniques. Very little guidance is available, requiring the incumbent to carry out these duties in a highly original and

collaborative fashion, often involving several groups and teams, as well as a variety of other internal and external customers/stakeholders.

Factor 5. Scope and Effect: Level 5-6, 450 Points

The purpose of the work is to address day-to-day privacy and other management issues and to generate solutions to critical problems by developing methods, tools, and strategies. Recommendations made may result in policy or procedural changes or revised program emphasis on bureau-wide privacy policies, guidelines, and procedures. The responsibilities of the incumbent are critical to compliance with Government privacy protection requirements related to information systems, websites, new technology, and paper file systems. They are also critical in ensuring that bureau and Departmental interests are addressed in intra- and inter-governmental privacy interests. Assignments are of major importance to each of several departments and agencies. Studies frequently involve extensive problems of coordination in fact-finding and in reviewing and testing recommendation in interested agencies or with outside groups.

Failure to manage privacy issues could and has made the bureau and the Department vulnerable to civil and criminal penalties, and censure by Congress and privacy advocate groups. Appropriate privacy protections relating to E-Government initiatives are essential for success of these projects to secure public and employee confidence in use of E-Government solutions. Noncompliance with OMB and statutory requirements can jeopardize the bureau's and the Department's ability to meet its fiduciary responsibilities or obtain funding for major projects if budget submissions do not meet OMB standards. This will adversely impact the ability of the bureau and the Department to accomplish its mission.

The bureau's activities are subject to constant controversy and scrutiny from all sources, including the national and local new media, and various interest groups (such as non-Government Privacy Advocacy groups). Privacy concerns in IT programs are highly visible and involve sensitive components of the bureau's and the Department's missions.

Factor 6, Personal Contacts and Factor 7, Purpose of Contacts: Level 4D, 330 Points

Personal Contacts:

Extensive personal contacts are required with executive officials and staffs at all organizational levels of the bureau and the Department. Incumbent has direct liaison with officials at OMB, Government-wide committees, intergovernmental organization as well as liaison and collaboration with stakeholder groups and senior federal official. The incumbent maintains regular contact with interested national and local professional organizations, industry and interest groups, and other non-governmental organizations. Other contacts vary widely and include all levels of the Department, counterparts in other Federal, state and Tribal organizations, private sector officials, Congressional representatives, law firms, and members of the general public. Contacts may be in person, by telephone, paper or electronic correspondence or any combination of these methods.

Contacts are made to plan, coordinate, advise, secure, direct or influence others against significant issues and to resolve problems and mutual concern. The incumbent must represent and defend the bureau's position on various planning process aspects concerning privacy within and outside the bureau. The incumbent proposes solutions and mediates differing objectives into mutually beneficial courses of action to gain acceptance of ideas or to achieve compliance with established policies and regulations.

Contacts serve to justify or settle matters involving significant or controversial issues, coordinate work, discuss issues, exchange information, resolve problems, explain policy positions, make recommendations, and negotiate differences in matters concerning the other areas of program responsibility. The incumbent must frequently present and defend analyses and recommendations in meetings with individuals and organizations with conflicting priorities. The incumbent may negotiate matters and may make commitments within his/her area of responsibility.

Contacts with the Department and other bureaus are largely to resolve issues, acquire input from customers, and obtain or provide needed information. Personal contacts also are to maintain knowledge or current techniques in the natural resources management, IT and associate professions as they relate to records issues. Public contacts usually involve coordination and information gathering, as well as explaining department programs and policies or facilitating the building of consensus positions on issues from several divergent and conflicting advocates or groups.

Factor 8. Physical Demands: Level 8-1, 5 Points

The work is mostly sedentary. Some travel is required, both within and outside the local commuting area. Occasional travel may be required to field activities for compliance review, determination of activity performance, and to conduct training and/or technical assistance. The incumbent must be able to function well under stressful conditions, often working under very tight deadlines involving projects of national significance.

Factor 9. Work Environment: Level 9-1, 5 Points

Work is performed primarily in office areas, conference rooms, and similar environments. No hazardous conditions are anticipated.

TOTAL POINTS = 4090 = GS-15
POINT RANGE = 4055 and above