

The Data Stewardship Program

DS022: Personally Identifiable Information (PII) Breach Policy

PURPOSE

This update to DS-22 improves the Census Bureau's Data Breach Response Committee (DBRC) procedures for handling moderate and high-level personally identifiable information (PII) breaches. It clarifies the responsibilities of Division Chiefs and department heads, and coordinates communications between the DBRC, senior managers, the Associate Directors, the Chief Operating Officer, and the Department of Commerce's Chief Privacy Officer.

Note: The mitigation of moderate or high-level PII breaches is the focus of this policy. Although data breaches involving business identifiable information (BII), Privacy Act protected information, and Title 13 and Title 26 data must still be reported to the BOC CIRT as required, these types of incidents and data breaches are out of scope for this policy unless they involve the compromise of PII. In addition, low-level PII breaches will continue to be handled by the Policy Coordination Office and are out of scope for this policy. PII incidents (distinct from PII breaches) are also out of scope. The second section of this policy contains a list of definition of commonly used PII breach related terms.

This policy rescinds DS-22A "Addendum to DS-22 Data Breach Policy."

SCOPE

The policy applies to a breach of PII/BII, which is a type of incident. For the purposes of this policy, the definitions in this section apply.

Definition of an Incident: An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. For example, an unencrypted email message containing sensitive PII that was blocked from transmission by the Census' Data Loss Prevention Email Scan (DLP) would be a PII incident, not a breach, since the unencrypted email was prevented from transmission by the DLP. Senior agency managers will be notified of PII *incidents*; however, the Census Bureau's DBRC will not be convened for these types of incidents.

Definition of a Breach: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. This includes a breach in any medium or form, including paper, oral, and electronic.

DS022 Personally Identifiable Information (PII) Breach Policy

A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PII by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include PII or portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PII for other than authorized purpose.

Some common examples of a breach include:

- A laptop or portable storage device storing PII is lost or stolen;
- An email containing PII is inadvertently sent to the wrong person;
- A box of documents with PII is lost or stolen during shipping;
- An unauthorized third party overhears agency employees discussing PII about an individual seeking employment or Federal benefits;
- A user with authorized access to PII data sells it for personal gain or disseminates it to embarrass an individual;
- An IT system that maintains PII is accessed by a malicious actor; or
- PII that should not be widely disseminated is posted inadvertently on a public website.

Business Identifiable Information (BII): information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person and privileged or confidential.” Commercial or financial information is considered confidential if disclosure is likely to cause substantial harm to the competitive position of the person from whom the information was obtained.

Classified Information: information that Executive Order 13526, “Classified National Security Information,” December 29, 2009 (3 CFR, 2010 Comp., p. 298), or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, requires agencies to mark with classified markings and protect against unauthorized disclosure.

Controlled Unclassified Information (CUI): information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see definition above) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.

Corrective/Remedial Actions: steps taken to mitigate losses and protect against any further breaches.

Enterprise Security Operations Center (ESOC): the organization that provides the Department of Commerce with cybersecurity status information and decision-making regarding cyber threat risks of various types.

Harm: any adverse effects that would be experienced by an individual whose sensitive PII was the subject of a breach, as well as any adverse effects experienced by the organization that maintains the PII. Harm to an individual includes any negative or unwanted effects (i.e., anything that may be socially, physically, or financially damaging). Examples of types of harm to individuals include, but are not limited to, the potential for blackmail, identity theft, physical harm, discrimination, or emotional distress. Organizations may also experience harm as a result of a loss of sensitive PII maintained by the organization, including but not limited to administrative burden, financial losses, loss of public reputation and public confidence, and legal liability.

Major Incident: an incident requiring a report to Congressional Committees no later than seven (7) days after the Department has considered the totality of the risk posed to the Department or Bureau/Operating Unit (BOU) and individuals and concluded a major incident has occurred. Incidents are considered major when:

The information involved is Classified, Controlled Unclassified Information (CUI), or PII; the incident resulted in the loss of critical service availability for all users or for at least 10,000 users, for eight hours or more; and the potentially compromised information poses a risk of harm to the Department or BOU and individuals.

The CIO shall document a determination that potentially compromised information does not pose a risk of harm to the affected organizations and individuals as well as any risk mitigations in place.

Or

The information involved is Classified, CUI, or PII; the incident resulted in the unauthorized modification, deletion, exfiltration of, or access to any records:

- related to 10,000 or more individuals;
- compromised or likely to result in a significant impact to Census Bureau's mission, public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence;
- the potentially compromised information poses a risk of harm to the affected organizations and individuals.

The CIO shall document a determination that potentially compromised information does not pose a risk of harm to the Census Bureau and individuals, as well as any risk mitigations in place.

Need to Know: information or data that is restricted due to its sensitive nature and the information is only given when needed or authorized.

Personally Identifiable Information (PII): information that is linked or linkable to a specific individual, and that can be used to distinguish or trace an individual's identity, either when used alone (name, Social Security number (SSN), biometric records, etc.)--or when combined with other personal or identifying information, (date and place of birth, mother's maiden name, etc.).

Sensitive PII is personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Some forms of PII are sensitive as stand-alone data elements. Examples of such PII include: SSN, driver's license or state identification number, passport number, Alien Registration Number, or financial account number. SSNs including truncated SSNs revealing only the last four digits are considered sensitive PII, both stand-alone and when associated with any other identifiable information.

Other data elements such as citizenship or immigration status; medical information; ethnic, religious, sexual orientation, or lifestyle information; and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also sensitive PII.

Additionally, the context of the PII may determine whether it is sensitive, such as a list of names of employees with poor performance ratings.

Risk: the level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. [NIST FIPS 200].

- Low is defined as the loss of confidentiality, integrity, or availability that is expected to have a limited adverse effect on organizational operations, organization assets or individuals. Breach incidents may be defined as Low if there was no failure of a Commerce IT security control, such as, an individual exposed his/her own sensitive PII.
- Moderate is defined as the loss of confidentiality, integrity, or availability that is expected to have a serious adverse effect on organizational operations, organization assets or individuals.
- High is defined as the loss of confidentiality, integrity, or availability that is expected to have a severe or catastrophic adverse effect on organizational operations, organization assets or individuals.

Security Control: NIST FIPS 200 specifies the minimum security requirements for information and information systems supporting executive agencies of the federal government. It provides a risk-based process for selecting appropriate security controls from the Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53), based on system categorization of High, Moderate or Low. For the protection of PII, security controls may include password protection, data encryption, full-disk encryption, or "auto-wipe" and "remote kill" features that provide the ability to protect a lost device by remotely disabling accessibility to data.

Substitute Notification: a supplemental notification of an incident breach which keeps potentially affected individuals informed when there is insufficient contact information or a means by which affected individuals are informed collectively. A substitute notification consists of a conspicuous posting of the notification on the home page of the Department's website and/or notification to major print and broadcast media, including major media in areas where the potentially affected individuals reside. Substitute notification includes phone numbers and email for affected individuals to use.

POLICY

1. ROLES AND RESPONSIBILITIES

The Data Breach Response Committee will consist of the following permanent members:

- Chief Operating Officer or designated senior agency official;
- Chief Privacy Officer;
- Chief, Privacy Compliance Branch;
- Associate Director for Information Technology and Chief Information Officer;
- Associate Director for Communications;
- Chief Financial Officer;
- Chief of the Public Information Office;
- Office of General Counsel; and
- Chief Administrative Officer.

The Policy Coordination Office's Chief of the Privacy Compliance Branch will assist the Chief Privacy Officer with coordinating meetings as appropriate. Other divisions/offices will be asked to participate, as warranted, including: Chief Information Security Officer and/or Chief of the Office of Information Security; Chief of the Office of Security; Chief of the Office of Congressional and Intergovernmental Affairs; and Office of the Inspector General.

In addition to those noted above, the Division/Office Chief or senior manager of where the incident occurred may be required to attend a DBRC meeting to: discuss the specific details of the incident; help to formulate an appropriate response; and assist in executing the breach response. The DBRC, or a designated representative, may also work closely with other Federal agencies, Bureaus, or teams to share lessons learned or to help develop government-wide guidance for handling PII data breach incidents. It is the role of each DBRC member to ensure there is complete and accurate reporting of all suspected PII data breach incidents, a full assessment is conducted, and then timely and appropriate responses are implemented.

Chief Privacy Officer

The Census Bureau's DBRC is chaired by the Census Bureau's Chief Privacy Officer (CPO). The CPO is responsible for providing guidance to the DBRC in establishing appropriate response to all PII breaches based on the specific characteristics of the incident, consistent with the guidance provided in the Department of Commerce's PII, BII, and PA Breach Response and Notification Plan, and OMB Memorandum M-17-12. The CPO holds the authority for convening the DBRC and overseeing related activities until closure of the PII breach. The CPO is the main

DS022 Personally Identifiable Information (PII) Breach Policy

point of contact for communication with the Census Bureau's Office of the Director, and the Department of Commerce's (DOC) Senior Agency Official for Privacy (SAOP).

Chief Information Officer

For PII breaches involving a cyber-security threat or breach, the Chief Information Officer (CIO), supported by the Chief Information Security Officer (CISO) or Chief of the Office of Information Security (OIS), is responsible for overseeing the completion of all cyber-security related activities and functions described in this policy. The CIO serves as the main point of contact with law enforcement agencies in cyber-security incidents and communications with the DOC's Enterprise Security Operations Center (ESOC).

Associate Director for Communications

The Associate Director for Communications (ADCOM), supported by the Chief of the Public Information Office (PIO), is responsible for public communication of the Census Bureau's PII incidents as appropriate. In addition, the ADCOM area will produce media talking points and a timeline of events surrounding the PII breach.

Other Committee Members

Tables 1 and 2 of this policy define the specific roles of each DRBC member.

When convened, the DBRC will have oversight of the following activities:

Assessing the Risk of Harm to Individuals Potentially Affected by a Breach - including the factors the agency shall consider when assessing the risk of harm to potentially affected individuals.

Mitigating the Risk of Harm to Individuals Potentially Affected by a Breach - including whether the agency should provide guidance to potentially affected individuals, purchase identity theft services for potentially affected individuals, and offer methods for acquiring such services.

Notifying Individuals Potentially Affected by a Breach - including if, when, and how to provide notification to potentially affected individuals and other relevant entities.

SPECIAL NOTE: The role and responsibilities of the Help Desk are currently out of scope for this document, however, they may be included later.

2. DELEGATION OF AUTHORITY

Each member of the DBRC shall participate in DBRC meetings when convened by the CPO and shall provide his/her expertise as needed to identify the best response for each PII data breach incident. Decisions and recommendations by the DBRC are made by consensus. When a consensus cannot be reached, the final decision will rest with the DBRC chair.

DS022 Personally Identifiable Information (PII) Breach Policy

If a DBRC member, a Division Chief, or an Associate Director is not available to participate in a meeting or provide input during a breach, his/her role must be delegated to someone at the same grade level or one level below.

3. COMPLIANCE

A key to compliance with the Data Breach Policy is effective and accurate communication. To ensure successful communication during a suspected or actual PII, BII, or PA data breach, all DBRC members must have a thorough understanding of the Department of Commerce's (DOC) PII breach notification plan, Census Bureau's data breach reporting and resolution processes, as well as, a full understanding of the roles and responsibilities of those directly involved in those processes.

Data Breach Response Committee Members

Each member of the DBRC must sign the attached Delegation of Authority and Compliance with DS-22 Agreement, stating that he/she has reviewed the DS-22 Data Breach Policy Addendum and fully understands his/her individual and collective roles and responsibilities.

The Census Bureau's Chief Privacy Officer (CPO) will maintain the signed agreement and ensure annual certification.

Division Chiefs and Office Chiefs

Each Associate Director is to ensure Division/Office Chiefs within his/her directorate receives a copy of this policy and sign the attached Acknowledge of Authority and Compliance with DS-22 Agreement.

Each DBRC member will maintain the signed agreement and ensure annual certification.

The roles and responsibilities of various units within the agency whenever a PII suspected and/or confirmed are detailed in Table 1.

Attachment A is the Delegation of Authority and Compliance with DS-22 Agreements to be signed by all members of the DBRC.

Attachment B is the Acknowledgment of Authority and Compliance with DS-22 Agreement to be signed by all Division/Office Chiefs.

Attachment C is the process flow and key communication points.

EFFECTIVE DATE

This policy is effective upon signature.

LEGAL AUTHORITIES

Office of Management and Budget (OMB) Memorandum M-17-12: *Preparing for and Responding to a Breach of Personally Identifiable Information*

Office of Management and Budget Circular Number A-130

Office of Management and Budget Memorandum M-16-24: *Role and Designation of Senior Agency Officials for Privacy*

OMB Memorandum M-06-16: *Protection of Agency Information*

NIST Special Publication 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*

Department of Commerce Breach Notification Plan

Department of Commerce Privacy Program Plan

Census Bureau Data Stewardship Policy *DS007: Safeguarding and Managing Information*

Census Bureau Data Stewardship Policy for *Notifying Management Officials of Employees Who Committed and Unauthorized Disclosure of Sensitive Personally Identifiable Information*

IMPLEMENTATION

Individuals and program areas will have responsibility for implementing this policy.

POLICY OWNER

The Chair of DSEP owns this policy.

SIGNATURE

By Direction:  Date: 2/22/18
Enrique Lamas,
Chair
Data Stewardship Executive Policy Committee

DS022 Personally Identifiable Information (PII) Breach Policy

Summary Information	
Policy Title:	DS022: Personally Identifiable Information (PII) Breach Policy
Date Signed:	February 22, 2018
Last Reviewed:	2018
Intended Audience:	All Staff
Policy Owner:	DSEP Chair (Chief Operating Officer)
Office Responsible for Implementation:	All Offices
Office Responsible for Dissemination:	All Offices
Stakeholder Vetting:	PCO, PPRC (representatives from ADCOM, ADITCIO, ADFO, ADEP, ADDP, ADDC, ORMPE, CDAR, CSM)

TABLE 1
Roles and Responsibilities for Implementing the Census Bureau Personally Identifiable Information Breach Policy

Role	Responsibility
Bureau of the Census	
Computer Incident Response Team (CIRT)	<ol style="list-style-type: none"> 1. Notifying the Chief Privacy Officer (CPO); Chief, Office of Information Security (OIS); Department of Commerce (DOC) CIRT; and US-CERT immediately of potential PII data loss/breach incidents according to reporting requirements. 2. Ensuring that the appropriate Property Management Office is notified of the breach when it involves computer or media storage. 3. Ensuring notification to the Office of Inspector General (OIG), when deemed necessary by the CIO or CPO. 4. Completing the weekly CIRT report.
Data Breach Response Committee (DBRC) Members	<ol style="list-style-type: none"> 1. Participating in DBRC meetings when convened by the CPO and providing subject matter expertise as needed to determine the best response for each incident. 2. Signing the <i>Delegation of Authority and Compliance with DS-22 Agreement</i>. 3. Conducting an in-depth risk analysis to determine the appropriate response to PII data breach incidents that may cause harm to individuals or the BOC. 4. Recommending the action to be taken, based on the risk score and other factors associated with the PII data breach incident. 5. Recommending whether notification to any third parties (e.g., law enforcement, media and the public, financial institutions, Congress, Department of Justice (DOJ), etc.) is necessary. 6. Recommending the method and content of notification when notification is deemed appropriate and necessary by the Chief Operating Officer. 7. Preparing and submitting a report identifying the risk score associated with an incident and the follow-up action or response taken. 8. Maintaining a file of all documents (emails, letters, request for quotes, reports, etc.) created in response to the incident in a secure location that is accessible to all DBRC members and for responding to future incidents. 9. Working with Associate Director for Communications to develop a standardized set of communication guidelines so that when a PII data breach incident occurs, a communication policy is already in place and only the appropriate information is shared with the right parties. 10. Assessing trends in reported PII data breach incidents to identify potential actions to decrease or limit future occurrences; reporting results of the assessment to the Chief Operating Officer.

DS022 Personally Identifiable Information (PII) Breach Policy

Role	Responsibility
	<ol style="list-style-type: none"> 11. Holding lessons learned meetings with all stakeholders after each major PII data breach incident to review how effective the incident handling process was and to identify needed improvements to processes and practices. 12. Recommending changes to the BOC Data Breach Policy and Data Breach Implementation Guide. Any recommended changes by the DBRC will go through the normal channels for policy revisions.
<p>Chief Privacy Officer (CPO) (Fulfilling the function of the SAOP in OMB Memo M-17-12)</p>	<ol style="list-style-type: none"> 1. Reviewing copies of reports of all PII data breach incidents. 2. Reporting incidents rated as “moderate” or “high” to the Senior Agency Official, the DBRC, the Department of Commerce (DOC) CPO and the US CERT as soon as possible. 3. Determining whether and when to convene DBRC meetings based on the initial level of risk assigned. 4. Determining who, in addition to regular members, needs to attend the DBRC meeting. 5. Serving as chair of the DBRC and signing the <i>Delegation of Authority and Compliance with DS-22 Agreement</i>. 6. Recommending a response plan to the Chief Operating Officer to mitigate risks to the individual(s) and to the BOC. 7. Following up and ensuring effective execution of the BOC’s response to each moderate or high rated PII data breach incident. 8. On an annual basis, ensuring all required staff sign the <i>Delegation of Authority and Compliance with DS-22 Agreements</i> and maintaining the signed document. 9. Meeting with the Senior Agency Official and DOC CPO to review reports on PII incidents/breaches. 10. Working closely with other Federal agencies, Bureaus or teams to share lessons learned or to help to develop government wide guidance for handling PII data breach incidents. 11. Being the point of contact when interacting with OIG.
<p>Policy Coordination Office (PCO) Privacy Compliance Branch Chief</p>	<ol style="list-style-type: none"> 1. Investigating PII data breach incidents in accordance with Census Bureau and DOC policies and procedures. 2. Providing a report of the results of its investigation to the DBRC and the DOC CPO, in accordance with reporting requirements. 3. Maintaining thorough records of PII data breach incidents from initial report through completed response. 4. Providing monthly (or as needed) reports about the DBRC’s activities to the CPO. 5. Assigning an initial rating level of the risk of harm for each PII data breach reported to BOC CIRT using the guidance in the Data Breach Implementation Guide. 6. Providing daily PII Breach reports to the CPO; immediately informing CPO of “moderate” or “high” rated PII breaches. 7. Working with the reporting area to determine the appropriate response to data breaches. 8. Resolving all “low” rated PII breaches.

DS022 Personally Identifiable Information (PII) Breach Policy

Role	Responsibility
	<ol style="list-style-type: none"> 9. Providing training and information on the PCO’s Intranet site on identifying PII data breaches and how to report incidents via the BOC CIRT. 10. Providing training to BOC CIRT Help Desk regarding the handling of PII data breach response as needed. 11. Developing and providing privacy related content for the annual data stewardship awareness training. 12. Updating policies and training, as appropriate, in response to problems identified by a specific event or identified trends. 13. Revising privacy policies when appropriate and getting the proper approvals on any changes. 14. Supporting the DBRC as appropriate. Managing the PII Incident Notification System (PINS) and ensuring appropriate managers are informed.
<p>Chief, Office of Information Security (OIS)</p>	<ol style="list-style-type: none"> 1. Managing the basic reporting functions of the BOC CIRT and working with the Network Operations Center (NOC) to ensure an available 24-hour contact channel for reporting potential PII data breach incidents. 2. Ensuring the Privacy Compliance Branch Chief is immediately notified of “moderate” or “high” rated PII breaches reported to the BOC CIRT. 3. Establish incident logging standards and review procedures for BOC CIRT and Security Operations Center (SOC) to ensure that adequate information is collected by logs and security software and that the quality of the data that is collected meets expectations. 4. Ensuring timely notification of PII incidents involving cyber-security to U.S. CERT. 5. Receiving reports of all PII data breach incidents from BOC CIRT. 6. Performing a daily review of all incidents reported to BOC CIRT to determine which incidents should be investigated as PII data breaches and providing a recommendation to the CPO. 7. Providing updates to the CPO regarding the BOC CIRT response to each PII data breach incident. 8. Providing information technology guidance in responding to suspected or known PII data breaches, such as an evaluation of controls or computer forensics investigation and analysis. 9. Serving as a member of the DBRC and signing the <i>Delegation of Authority and Compliance with DS-22 Agreement</i>. 10. Working with affected Divisions/Offices, to take IT security steps to control and contain the PII data breach, including: <ul style="list-style-type: none"> • monitoring, suspending, or terminating, as appropriate, affected accounts, • modifying computer access or physical access controls, and • taking other necessary and appropriate action without undue delay and consistent with current requirements under FISMA. 11. Assessing trends in reported incidents and identifying potential actions to decrease or limit occurrences. 12. Providing training and information on the OIS intranet site on identifying PII data breach incidents and how to report incidents to the BOC CIRT. 13. Overseeing the completion of all PII breach cyber-security related activities. 14. Coordinating with outside law enforcement agencies as appropriate.

DS022 Personally Identifiable Information (PII) Breach Policy

Role	Responsibility
	15. Communicating with the DOC's Enterprise Security Operations Center as appropriate.
Senior Agency Official (SAO) (i.e., Chief Operating Officer or designated senior agency official)	<ol style="list-style-type: none"> 1. Meeting weekly with the CPO to review all PII data breach incident reports and recommendations from the DBRC. 2. Reviewing recommendations made by the DBRC and determining which incidents referred by the DBRC warrant investigation as PII data breaches. 3. Assessing whether the breach response action recommended by the CPO should be taken by the Agency. 4. Issuing the notice of breach, as appropriate. 5. Serving as a member of the DBRC and signing the <i>Delegation of Authority and Compliance with DS-22 Agreement</i>.
Associate Director and/or Division/Office Chief Where Breach Occurred/Was Reported (will vary by incident) (AD_BO)	<ol style="list-style-type: none"> 1. Ensuring employees within the directorate are familiar with the PII breach reporting requirements. 2. Establishing internal processes within the directorate, consistent with BOC policies and procedures, for handling a suspected or confirmed PII data breach incident. 3. Providing appropriate information, documentation, and training to staff within the directorate to prevent and deter future PII data breach incidents. 4. Signing the <i>Acknowledge of Authority and Compliance with DS-22 Agreement</i> and maintaining copies in with the Associate Director's Office. 5. Identifying individuals within the directorate that should be a part of the initial BOC CIRT notification of reported PII data breach incidents. 6. Identifying individuals within the directorate who should be on the email chain once a PII data breach incident has been identified and/or confirmed. 7. Participating in DBRC meetings, when invited, to discuss: the specific details of the incident; the determination of the risk level for the incident; the formulation of an appropriate response; and assisting in executing the BOC's breach response. 8. Assisting the DBRC, or others offices as appropriate, with investigating a suspected PII data breach incident. 9. Providing full documentation to the CPO and DBRC of any mitigation steps taken and future plans to mitigate or prevent reoccurrence within the directorate. 10. Participating in any follow-up meetings with the DBRC regarding the PII data breach incident. 11. Reviewing and taking appropriate action on all PII breaches reported by through the PINS. 12. Working with HRD for ensuring appropriate administrative actions for employee(s) responsible for a PII data breach, if warranted.
Associate Director for Communications (ADCOM)	<ol style="list-style-type: none"> 1. Drafting materials to provide to the public, media, and/or those affected by the breach, as appropriate, and ensuring the notification is appropriately tailored to the nature and scope of the risk. 2. Acting as the single point of contact for interacting with outside groups and organizations, such as, the media, Congress, advisory committees, state and local authorities, tribal leaders, etc., regarding a PII data breach incident. 3. Coordinate public messaging with DOC-Office of Public Affairs (OPA)

DS022 Personally Identifiable Information (PII) Breach Policy

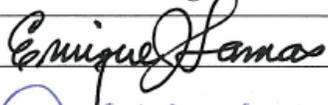
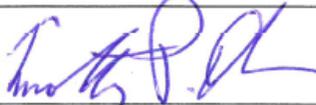
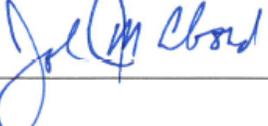
Role	Responsibility
	<ol style="list-style-type: none"> 4. Working with DOC Office of Legislative and Intergovernmental Affairs (OLIA) to coordinate all communications and meetings with members of Congress and their staff, regarding the breach. 5. Serving as a member of the DBRC and signing the <i>Delegation of Authority and Compliance with DS-22 Agreement</i> (Attachment A).
Chief Administrative Officer (CAO)/Human Resources Division (HRD)	<ol style="list-style-type: none"> 1. Working collaboratively with the PCO, ensuring new hires are provided training on the importance of the safe handling of data and how to identify and report potential PII data breaches as part of HRD's New Employee Orientation training. 2. Working with offices where a PII data breach occurred to advise managers on appropriate disciplinary action for employees responsible for the breach, if warranted.
Chief, Office of Security (OSY)	<ol style="list-style-type: none"> 1. Participating as a member of the DBRC upon request. 2. Signing the <i>Delegation of Authority and Compliance with DS-22 Agreement</i>. 3. Being the point of contact when interacting with law enforcement, where needed. 4. Coordinating with ADCOM on all information regarding incidents for release to outside organizations. 5. Receiving incident reports on lost, missing, or stolen Digital Storage Media (<i>CD/DVD, Secure Digital or Memory Cards, Hard Drives, Flash Drives, etc.</i>), Electronic Hardware (Laptops, Smartphones, Tablets, Computer Workstations or Servers, Printers/Copiers, Remote Secure Access Tokens, etc.) Physical Security (ID Badge), and Paper Items (Current Surveys, Decennial Surveys, Other Paper) via the BOC CIRT. 6. Reviewing and investigating reported incidents with a focus on potential criminal activity and/or negligence, while the Policy Coordination Office (PCO) takes the lead on the PII data breach aspect of each case. 7. Providing information to PCO regarding OSY investigations as requested.
Employees/Contractors	<ol style="list-style-type: none"> 1. Knowing and adhering to the policies and requirements for safe data handling and PII breach/incident reporting. 2. Reporting incidents to the BOC CIRT as soon as possible, or no later than 1 hour of discovery. 3. Completing the required annual Data Stewardship Awareness Training.
Office of General Counsel (OGC)	<ol style="list-style-type: none"> 1. Providing legal support and guidance in responding to an incident and in developing policies and procedures.

Attachment A

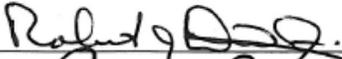
Delegation of Authority and Compliance with DS-22 Agreement

For Associate Directors and Data Breach Response Committee Members

As an Associate Director and/or member of the Data Breach Response Committee (DBRC), I acknowledge that I have read the DS-22, understand my role and responsibilities on the Committee as outlined in the Policy and agree to comply with implementing the Policy. If I am not available to participate in a meeting or provide input during a breach, I will delegate my role to a Division Chief or a GS-15.

Delegation of Authority and Compliance with DS-22, Data Breach Policy		
Name/Signature	Date	Area Representing
	6/29/18	Chief Operating Officer (COO)
	5/15/18	Chief Administrative Officer (CAO)
	6/11/18	Chief Financial Officer (CFO)
	5.15.18	Associate Director for Communications (ADCOM)
	6-28-18	Associate Director for Demographic Programs (ADDP)
	6-29-2018	Associate Director for Economic Programs (ADEP)
	6/1/2018	Associate Director for Field Operations (ADFO)
	5-15-18	Associate Director for Information Technology & Chief Information Officer (ADITCIO)
	6/5/18	Associate Director for Decennial Census Programs (ADDP)
	6/7/2018	Associate Director for Research & Methodology (ADRM)

DS022 Personally Identifiable Information (PII) Breach Policy

	6-6-18	Chief, Office of Security (OSY)
	6/5/18	Chief Privacy Officer (CPO)
	6/28/18	Chief, Office of Information Security (OIS)

Attachment B

Acknowledgment of Authority and Compliance with DS-22 Agreement

For Division/Office Chief

I acknowledge that I have read the DS-22 Data Breach Policy and understand my role and responsibilities on the Committee as outlined in the Policy. I am aware that if a data breach occurs in my area, I will need to participate on the DRBC and assist with the breach incident investigation. If I am not available to participate in a meeting or provide input during a breach, I will delegate my role to a GS-15.

Name (print)

Signature

Date

Division/Office

DS022 Personally Identifiable Information (PII) Breach Policy

Attachment C

Process for Handling PII Breaches

