DS-22 DATA BREACH POLICY
ADDENDUM

I. TITLE

Addendum to the DS-22 Data Breach Policy

II. PURPOSE/STATEMENT OF PROBLEM

Communication procedures in the current data stewardship Data Breach policy (DS-22) are lacking clear definitions and guidance on how to efficiently resolve high level data breaches involving personally identifiable information (PII). This addendum to DS-22 improves the procedures for handling high level PII breaches by establishing the function and role of the Census Bureau's Data Breach Response Committee (DBRC), laying out the responsibilities of Division Chief's and department heads, and organizing communications between the DBRC, senior managers, the Associate Directors, the Deputy Director, and the Department of Commerce's Chief Privacy Officer.

SPECIAL NOTE REGARDING IOE 6: In addition to the communication procedural issues with the current policy, the agency's adoption of IOE 6 introduced new procedures regarding the treatment of data breaches that have not been reconciled with the current DS-22 Data Breach Policy. The resolution of DS-22 and IOE 6 is a larger undertaking that will be addressed separately by the Privacy Policy Research Committee. This addendum serves to address the immediate communication problem with the handling of high level PII breaches and will remain in effect pending the revision of the DS-22 Data Breach Policy.

III. ROLES AND RESPONSIBILITES

The Census Bureau's DBRC is responsible for developing an appropriate response to all PII data breaches based on the specific characteristics of the incident, consistent with the guidance provided in the Data Breach Policy (DS-22) and the Policy's Implementation Guide. The DBRC will consist of the following permanent members: Deputy Director or designated senior agency official; Associated Director for Information Technology and Chief Information Officer; Associate Director for Communications; and the Chief Privacy Officer. The Policy Coordination Office's Chief of the Privacy Compliance Branch will coordinate meetings, as appropriate. Others divisions/offices will be asked to participate, as warranted, including: Chief of the Office of Information Security; Chief of the Office of Security; Office of General Counsel; and Office of the Inspector General.

In addition to those noted above, the Division/Office that initially reported a PII data breach incident might be asked 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.

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

IV. DELEGATION OF AUTHORITY

Each member of the DBRC shall participate in DBRC meetings when convened by the Chief Privacy Officer 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.

If a DBRC member, a Division Chief, or 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.

V. 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 data breach, all DBRC members must have a thorough understanding of Census Bureau's PII data breach reporting and resolution processes, as well as, a full understanding of the roles and responsibilities of those directly involved in those processes.

Associate Directors and Data Breach Response Committee Members

Each Associate Director 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 Associate Director will maintain the signed agreement and ensure annual certification.

The roles and responsibilities of various units within the BOC whenever a PII data breach is suspected and/or confirmed are detailed in Table 1. Table 2 summarizes responsibilities across areas.

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

Attachments (3)

TABLE 1
Roles and Responsibilities for Implementing the Bureau of the Census (BOC) Data Breach Policy

Role	Responsibility
Bureau of the Census	
Computer Incident Response Team (CIRT)	1. Notifying the Chief Privacy Officer (CPO); Chief, Office of Information Security (COIS; 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 necessary. 4. Completing the weekly CIRT report.
Data Breach Response Committee (DBRC) Members	1. Participating in DBRC meetings when convened by the Chair and providing Subject Matter Expert (SME) expertise as needed to determine the best response for each incident. 2. Signing the *Delegation of Authority and Compliance with DS-22 Agreement.* 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)) is necessary. 6. Recommending the method and content of notification when notification is deemed appropriate and necessary by the Director or Deputy Director. 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 Deputy Director. 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. 13. Establishing communications with persons who report a PII data breach.
Chief Privacy Officer (CPO)	1. Receiving copies of reports of all PII data breach incidents. 2. Reporting incidents rated as "moderate" or "high risk" to the Senior Agency Official, the DBRC, the Department of Commerce (DOC) CPO and the US CERT within one hour of notification by the BOC CIRT. 3. Determining whether and when to convene DBRC meetings based on the initial level of risk assigned. 4. Determining whom, in addition to regular members, needs to attend the DBRC meeting. 5. Serving as chair of the DBRC and signing the *Delegation of Authority and Compliance with DS-22 Agreement.* 6. Reporting PII data breach incidents to the DOC CPO, as required, based on the initial risk score. 7. Recommending a response plan to the Deputy Director to mitigate risks to the individual and to the BOC. 8. Following up and ensuring effective execution of the BOC's response to each moderate or high rated PII data breach incident. 9. On an annual basis, ensuring the *Delegation of Authority and Compliance with DS-22 Agreements* are signed by all required staff and maintaining the signed document. 10. Meeting biweekly with the Senior Agency Official and DOC CPO to review reports on PII incidents/breaches. 11. 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.
Policy Coordination Office (PCO)	1. Investigating PII data breach incidents in accordance with Census Bureau policy. 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. Performing a weekly review of all incidents reported through the BOC CIRT to determine which ones should be investigated as PII data breaches. 5. Providing monthly (or as needed) reports about the DBRC's activities to Senior Agency Officials, as determined by the CPO. 6. Assigning an initial rating level of the risk of harm for each PII data breach incident reported to BOC CIRT using the guidance in the Data Breach Implementation Guide. 7. Providing daily PII Breach reports to the CPO; immediately informing CPO of "moderate" or "high" incidents. 8. Working with the reporting area to determine the appropriate response to "low or medium risk" incidents. 9. Executing the response to PII data breach incidents rated not applicable, low, or medium in accordance with Census Bureau policy. 10. Providing training and information on the PCO's Intranet site on identifying PII data breaches and how to report incidents via the BOC CIRT. 11. Providing training to BOC CIRT regarding the handling of PII data breach response as needed. 12. Developing and providing privacy and data stewardship training. 13. Updating policies and training, as appropriate, in response to problems identified by a specific incident or trends indicated by several incidents. 14. Evaluating the initial PII data breach incident report and making the initial risk level determination. 15. Revising privacy policies when appropriate and getting the proper approvals on any changes. 16. Serving as a member of the DBRC and signing the *Delegation of Authority and Compliance with DS-22 Agreement*.
Chief, Office of Information Security (COIS)	1. Providing BOC CIRT capabilities. 2. Managing 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. 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. Receiving reports of all PII data breach incidents from BOC CIRT. 5. 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. 6. Providing updates to the CPO regarding the BOC CIRT response to each PII data breach incident. 7. 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.

	8. Serving as a member of the DBRC and signing the *Delegation of Authority and Compliance with DS-22 Agreement.* 9. Working with affected Divisions/Offices, to take steps to control and contain the PII data breach, including: • Monitoring, suspending, or terminating, as appropriate, affected accounts • Modifying computer access or physical access controls • Taking other necessary and appropriate action without undue delay and consistent with current requirements under FISMA. 10. Assessing trends in reported incidents to identifying potential actions to decrease or limit occurrences. 11. Providing training and information on the OIS intranet site on identifying PII data breach incidents and how to report incidents.
Senior Agency Official (SAO) (i.e., Deputy Director or designated senior agency official)	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 *Delegation of Authority and Compliance with DS-22 Agreement.*
Associate Director and/or Division/Office Chief Where Breach Occurred/Was Reported (will vary by incident) (AD_BO)	1. Ensuring timely reporting by employees within the directorate of any suspected or confirmed PII data breach incidents. 2. Establishing internal processes within the directorate, consistent with BOC policies and procedures, for handling a suspected or confirmed PII data breach incident. 3. Signing the *Acknowledge of Authority and Compliance with DS-22 Agreement* and maintaining copies in with the Associate Director's Office. 4. Identifying individuals within the directorate that should be a part of the initial BOC CIRT notification of reported PII data breach incidents. 5. Identifying individuals within the directorate who should be on the email chain once a PII data breach incident has been identified and/or confirmed. 6. 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. 7. Assisting the DBRC, or others offices as appropriate, with investigating a suspected PII data breach incident.

	8. Providing full documentation to the CPO and DBRC of any mitigation steps taken and future plans to mitigate or prevent reoccurrence within the directorate. 9. Participating in any follow-up meetings with the DBRC regarding the PII data breach incident. 10. Providing appropriate information, documentation, and training to staff within the directorate to prevent and deter future PII data breach incidents 11. Working with HRD for ensuring appropriate administrative actions for employee(s) responsible for a PII data breach, if warranted.
Associate Director for Communications (ADCOM)	1. Drafting breach notification 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. Coordinating notifications to individuals, the media and other third parties with other Agency staff. 3. Acting as the single point of contact for interacting with individuals, customers, the media and other third parties, regarding a PII data breach incident. 4. Working with DOC Office of Legislative and Intergovernmental Affairs (OLIA) to coordinates 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 *Delegation of Authority and Compliance with DS-22 Agreement*.
Human Resources Division (HRD)	1. Working collaboratively with the PCO, ensures 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 take appropriate administrative action for employees responsible for the breach, if warranted.
Chief, Office of Security (OSY)	1. Participating as a member of the DBRC upon request. 2. Signing the *Delegation of Authority and Compliance with DS-22 Agreement*. 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. Defining circumstances and timing for when employees, customers and partners may or may not be informed of the incident. 6. Receiving incident reports on lost, missing, or stolen Digital Storage Media *(CD/DVD, Secure Digital or Memory Cards, Hard Drives, Flash Drives)*, Electronic Hardware (Laptops, Smartphones, Tablets, Computer Workstations or Servers, Printers/Copiers, Remote Secure Access Tokens) Physical Security (ID Badge), and Paper Items (Current Surveys, Decennial Surveys, Other Paper) via the Data Breach System that can include a PII data breach component. 7. 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. 8. Providing information to PCO regarding OSY investigations as requested.
Employees/Contractors	1. Knowing the policies and requirements for safe data handling and proper and timely reporting of incidents to the BOC CIRT.
Office of General Counsel (OGC)	1. Providing legal support and guidance in responding to an incident.
Office of Inspector General (OIG)	1. Determining whether to notify the DOJ or other law enforcement authorities following a PII data breach. 2. Notifying and advising the DBRC about ongoing investigations and the timing of proposed external notifications that may affect such notifications.

Table 2: Summary Matrix Table of Responsibilities

Line No.	Responsibilities	CIRT	DBRC	CPO	PCO	ADIT-CIO	COIS	SAO	ADCOM	AD_BO	HRD	OSY	OGC	OIG
1	Permanent member of the DBRC			X	X	X		X	X					
2	Completing the weekly CIRT report	X												
3	Notifying the Chief Privacy Officer (CPO), DOC CIRT and US-CERT of potential PII data breach incidents according to reporting requirements	X			X									
4	Receiving and investigating all PII data breach incidents in accordance with BOC policy				X									
5	Conducting and or/participating an in-depth risk analysis, identifying the risk score associated with an incident	X	X	X	X	X	X		X	X				
6	Providing a report of the results of the investigation and the follow-up action or response taken. to the appropriate entities as defined in the Data Breach Implementation Guidelines		X	X	X									
7	Ensuring that the appropriate Property Management Office is notified of the breach when it involves computer or media storage	X												
8	Ensuring notification to the OIG, when necessary	X	X	X	X	X	X							
9	Recommending what action to take based on the risk score and other factors associated with the breach.		X	X	X	X								
10	Recommending whether notification to any third parties (e.g., law enforcement, media and the public, financial institutions, Congress, DOJ) is necessary.		X	X		X	X	X	X			X		
11	Filing all documents (emails, letters, request for quotes, etc.) created in response to the incident in a secure location that is accessible to all DBRC members and for responding to future incidents.	X	X											

Line No.	Responsibilities	CIRT	DBRC	CPO	PCO	ADIT-CIO	COIS	SAO	ADCOM	AD_BO	HRD	OSY	OGC	OIG
12	Participating in DBRC meetings when convened by the Chair and providing SME expertise as needed to provide the best response for each incident.		X	X	X									
13	Developing pre-determined communication guidelines so that when a breach occurs, only the appropriate information is shared with the right parties.		X	X	X				X					
14	Establishing communications with the person who reports a breach or improper disclosure of Title 26 federal tax information (which should be reported directly to the Treasury Department and not BOC CIRT)		X	X	X	X								
15	Holding lessons learned meeting with all stakeholders to review how effective the incident handling process was after each major data breach incident and identify needed improvements to processes and practices.		X	X	X	X								
16	Working closely with other Federal agencies, offices or teams to share lessons learned or help to development government wide guidance for handling PII data breach incidents		X	X	X	X								
17	Recommending changes to the BOC Data Breach Policy and Data Breach Implementation Guide		X	X	X	X	X	X	X	X	X	X	X	X
18	Performing a weekly review of all PII incidents reported through to CIRT to determine which ones should be investigated as breaches and providing a report to the Senior Agency Official				X									
19	Assessing trends in reported PII incidents to identifying potential actions to decrease or limit			X	X									

Line No.	Responsibilities	CIRT	DBRC	CPO	PCO	ADIT-CIO	COIS	SAO	ADCOM	AD_BO	HRD	OSY	OGC	OIG
	occurrences													
20	Serving as chair of the DBRC			X										
21	Providing regular reports about the DBRC activities to Senior Census Bureau Officials			X										
22	Assigning an initial rating level of the risk of harm for each PII data breach incident using the guidance in the Data Breach Implementation Guidelines	X			X									
23	Determining whether and when to convene DBRC meetings based on the initial level of risk assigned			X										
24	Determining who, in addition to regular members, needs to attend the DBRC meeting		X	X		X								
25	Determining the necessity for notification and, if warranted, notifying Senior Agency Officials after the initial assessment and rating of the incident		X	X										
26	Recommending a response plan to the Senior Agency Official to mitigate risks to the individual and the DOC			X	X	X								
27	Following up and ensuring effective execution of each breach response			X	X									
28	Maintaining thorough records of PII data breach incidents from initial report to BOC CIRT through completed response.			X	X									
29	Providing training and information on its Intranet site on identifying and reporting breaches via the CIRT.			X	X		X			X				
30	Providing training to staff on the importance of safe handling of data to prevent and deter breach incidents, and how to identify and report potential breaches				X					X	X			
31	Providing BOC CIRT capabilities						X							

Line No.	Responsibilities	CIRT	DBRC	CPO	PCO	ADIT-CIO	COIS	SAO	ADCOM	AD_BO	HRD	OSY	OGC	OIG
32	Providing training to BOC CIRT regarding the handling of PII data breach response as needed			X	X		X							
33	Recommending updates to policies and training as appropriate in response to problems identified by a specific incident or trends indicated by several incidents		X	X	X	X	X	X	X	X	X	X	X	X
34	Providing a report to Senior Agency Officials (the Director and Deputy Director) as necessary			X	X									
35	Reporting PII data breach incidents to the DOC CPO as required based on the initial risk score.			X	X									
36	Coordinating the response to PII data breach incident rated moderate or high with the DOC CPO			X	X									
37	Executing the breach response to PII data breach incidents rated not applicable or low				X									
38	Providing information technology guidance in responding to suspected or known breaches, such as an evaluation of controls or computer forensics investigation and analysis					X	X							
39	Working with the affected bureau/office, to take appropriate steps to control and contain the breach			X	X									
40	Reviewing incident reports and determining which incidents referred by the DBRC warrant investigation as breaches			X	X									
41	Issuing the official notice of a breach			X	X			X						
42	Participating in DBRC meetings, when invited, to discuss the specific details of the incident, help to formulate an appropriate response and assist in executing the breach response.									X	X	X	X	X

Line No.	Responsibilities	CIRT	DBRC	CPO	PCO	ADIT-CIO	COIS	SAO	ADCOM	AD_BO	HRD	OSY	OGC	OIG
43	Ensuring timely reporting by employees of any suspected or confirmed breach incidents									X				
44	Establishing internal processes for handling a breach				X		X			X		X		
45	Establish logging standards and procedures to ensure that adequate information is collected by logs and security software and that the quality of the data that is input is reviewed regularly	X					X							
46	Identifying individuals within the directorate/office that should be a part of the initial BOC CIRT notification				X		X			X		X		
47	Identifying individuals who should be on email chain once a breach has been identified				X		X			X		X		
48	Assisting the OIS in the investigation of any suspected IT breach incident.			X						X				
49	Providing full documentation of any mitigation steps taken and future plans to mitigate or prevent reoccurrence within the directorate									X				
50	Participating in any follow-up meetings with the DOC regarding the breach incident									X				
51	Taking appropriate administrative action for employees responsible for data breach, if warranted.									X	X			
52	Recommending the method and content of notification when notification is deemed appropriate and necessary by the Senior Agency Official.		X	X					X			X		
53	Drafting notification of the breach to the public, media, and/or those affected by the breach, as appropriate, tailoring the notification to the nature and scope of the risk								X					

Line No.	Responsibilities	CIRT	DBRC	CPO	PCO	ADIT-CIO	COIS	SAO	ADCOM	AD_BO	HRD	OSY	OGC	OIG
54	Coordinating notifications to individuals, the media and other third parties								X					
55	Acting as single point of contact for interacting with customers and media regarding a data breach incident.								X					
56	Working with DOC OLIA to coordinates all communications and meetings with members of Congress and their staff regarding the breach (b-4)								X					
57	Being the point of contact when interacting with law enforcement, where needed											X		
58	Providing legal support and guidance in responding to an incident												X	
59	Determining whether to notify the DOJ or other law enforcement authorities following a breach												X	X
60	Notifying and advising the DBRC about ongoing investigations and the timing of proposed external notification that may affect such notifications.												X	X

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**
Nancy Potok / Nancy Potok	3/6/14	Deputy Director
[signature]	5/27/14	Associate Director of Administration & ADACFO (ADACFO)
[signature]	5/12/14	Associate Director for Communications (ADCOM)
[signature]	5/13/14	Associate Director for Decennial Programs (ADDC)
Enrique Lamas	5/12/14	Associate Director for Demographic Programs (ADDP)
William Bostic Jr. / William Bostic Jr.	4/28/14	Associate Director for Economic Programs (ADEP)
William W. Hatcher / William W. Hatcher	5/27/14	Associate Director for Field Operations (ADFO)
[signature]	5/6/14	Associate Director for Information Technology & CIO (ADITCIO)
[signature]	5/13/14	Associate Director for 2020 Census (AD20C)
Thomas A Louis	5/13/14	Associate Director for Research & Methodology (ADRM)
		Chief Privacy Officer (CPO)

Attachment B

Acknowledgment of Authority and Compliance with DS-22 Agreement

For Division/Office Chief

I acknowledge that I have read the DS-22 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.

Nancy Potok
Name (print)

Nancy Potok
Signature

2/26/14
Date

Dep. Dir
Division/Office

Attachment C

Process for Handling PII Breaches

Process for Handling PII Breaches