THE WHITE HOUSE

WASHINGTON

February 11, 2014

MEMORANDUM FOR THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF COMMERCE
THE SECRETARY OF ENERGY
THE SECRETARY OF HOMELAND SECURITY
DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY
ADMINISTRATOR OF THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
DIRECTOR OF THE OFFICE OF PERSONNEL MANAGEMENT
DIRECTOR OF THE NATIONAL SECURITY AGENCY
DIRECTOR OF THE DEFENSE INTELLIGENCE AGENCY
ADMINISTRATOR OF THE DRUG ENFORCEMENT ADMINSTRATION
DIRECTOR OF THE INFORMATION SECURITY OVERSIGHT OFFICE

SUBJECT: Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures

In response to the WikiLeaks disclosures in 2010, the President issued Executive Order (E.O.) 13587 directing structural reforms to improve the security of classified information on computer networks. This order established the Senior Information Sharing and Safeguarding Steering Committee ("Steering Committee"), made up of representatives from throughout departments and agencies, to set government-wide reform goals and oversee implementation by all United States Government components that handle classified information.

In 2012, the Steering Committee established its initial priorities as: (1) mitigating risks inherent to removable media, (2) reducing anonymity, (3) establishing insider threat programs, (4) improving access control, and (5) enhancing enterprise audit. It is essential that departments and agencies complete their efforts to reach full operating capability in each of these areas, particularly in establishing their insider

threat programs in accordance with the President's National Insider Threat Policy and Minimum Standards.

Recent unauthorized disclosures have unfortunately underscored the need to vigilantly safeguard our Nation's most sensitive intelligence information. Informed by these recent disclosures, I directed the Steering Committee to develop near-term measures, beyond those already planned under E.O. 13587, aimed at further reducing the risk of additional high-impact disclosures. In the course of that process, the Steering Committee concluded that technical fixes alone cannot fully mitigate the threat posed by a determined insider. As a result, the Steering Committee's recommendations, which are detailed in Tab A, include measures to improve business practices, enhance the security culture across the workforce, and reduce the unique risks associated with "privileged" users.

Separately, following the incident at the Washington Navy Yard in September 2013, the President asked the Director of the Office of Management and Budget (OMB) to lead a 120-day review of Federal employee suitability and contractor fitness determinations, as well as security clearance procedures. This review will come to a close at the end of February. In the course of these parallel reviews, the National Security Council staff coordinated closely with OMB to ensure the recommendations were appropriately aligned. While these efforts were underway, the President's Review Group on Intelligence and Communications Technologies also published its report and recommendations, a number of which address information and personnel security.

The 45-day review, the 120-day review, and the President's Review Group produced largely complementary recommendations. Of note, all three recommended implementing personnel security continuous evaluation. That work is ongoing within the Office of the Director of National Intelligence and the Department of Defense, under the oversight of the Suitability and Security Clearance Performance Accountability Council.

With the completion of the 45-day review, and keeping in mind the complementary work that will be undertaken as a result of the 120-day review and Review Group recommendations, I request recipient department and agency heads to proceed with implementing the measures specified in Tab A. These efforts should be completed no later than December 31, 2014, and within your agency's overall resource levels. The corrective measures are applicable to any classified computer network that contains particularly sensitive information at any level of

classification, including special access programs; intelligence sources, methods, and activities; and operational details affecting law enforcement, military, and diplomatic operations. As needed, the Classified Information Sharing and Safeguarding Office will provide more detailed guidance on implementing these measures.

To ensure these measures are also implemented by private sector entities that are approved to handle classified information, the Director of the Information Security Oversight Office will develop and promulgate necessary implementation guidance pursuant to E.O. 12829 under the National Industrial Security Program.

Consistent with the President's guidance, department and agency heads should be personally involved in driving ongoing reforms and implementing these new near-term measures. Many agencies have already begun implementing the actions identified by the Steering Committee and we support those ongoing efforts. Departments and agencies should continue to provide quarterly progress reports on the Key Information Sharing and Safeguarding Indicators through the established process. I also ask that you ensure each quarterly report submitted by your designated insider threat program senior official is consistent with your guidance.

Thank you for prioritizing the implementation of these measures.

Lisa O. Monaco
Assistant to the President for
Homeland Security and Counterterrorism

Attachment
Tab A Near-term Measures for Implementation

Tab A

Near-term Measures for Implementation

Task Group A: Personnel Security and Management		
Task	*Responsible Entity*	*Suspense*
A-1. Conduct a review of all privileged users[1] to ensure they have a continuing need for privileged capabilities or access. Ensure they have current security clearances and minimize any granted exceptions.[2]	All Recipient D/As	6/30/2014
A-2. DNI will lead a privileged access steering group to develop a risk-based approach to identify and assess users with extraordinary[3] access to particularly sensitive information.[4] This approach will consider both the degree and duration of potential harm that can be caused by the user's access.	ONCIX and IC-CIO	6/30/2014
A-3. DNI shall develop and launch a personnel Continuous Evaluation Program (CEP) that includes automated checks of designated government and commercial databases and records sources[5] as well as the analytical tools necessary to flag issues above predefined thresholds. The CEP shall reach initial operating capability[6] by September 30, 2014, with participation of the Intelligence Community (IC) elements in the eight listed departments and agencies. DNI, in his role as the Executive Agent for Security, will develop the necessary plans and timetables for expanding the implementation of CEP across the government, consistent with the recommendations of the forthcoming 120-Day Suitability and Security Report to the President.	DNI with CIA, DIA, DOD, FBI, NGA, NRO, NSA, and State	9/30/2014
A-4. OPM, DNI, and the NITTF will convene a group of security and human resources professionals from relevant departments and agencies to develop a security and insider threat performance element to be incorporated into the performance plans of all IC employees beginning in FY15. The group shall consider the effectiveness of and adherence to the existing requirement in E.O. 13526 section 5.4(d)(7). Other agencies shall implement similar changes for relevant employees, such as those with access to DOD Special Access Programs and DOE Restricted Data.	OPM and DNI	9/30/2014
A-5. DNI will develop a standardized security and insider threat awareness training module for mandatory IC-wide use beginning in FY15. This training shall meet the requirements set forth in Section I.1-3 of the Insider Threat Minimum Standards. DNI shall make this training module available to other agencies upon request.	DNI	9/30/2014

A-6. Each insider threat senior official shall attend one senior official event sponsored by the National Insider Threat Task Force during FY14.	All Recipient D/As	9/30/2014

[1] Reference DNI executive correspondence (E/S 00514) of July 25, 2013 regarding "Oversight of Privileged users within the Intelligence Community" which defines the term "privileged user" for the purpose of this tasking.
[2] An "exception" is an adjudicative decision to grant initial or continued access eligibility despite a failure to meet the full adjudicative or investigative standards. See also ICPG 704.4, H.1.
[3] "Extraordinary" access means significantly greater access to multiple special or compartmented programs and data repositories than average network users.
[4] "Particularly sensitive information" includes that protected by special access programs; that which might reveal intelligence sources, methods, or activities; and operational details affecting law enforcement, military, or diplomatic operations.
[5] Subject to necessary legal review.
[6] Initial Operating Capability is defined by the Security Executive Agent CEP Concept of Operations plan.

Task Group B: Data Management		
Task	*Responsible Entity*	*Suspense*
B-1. Conduct a review of all information sharing portals[7] hosted on classified computer networks to ensure each requires authentication and supports enterprise audit.[8] Non-compliant portals shall be appropriately secured or removed.	All Recipient D/As	6/30/2014
B-2. Conduct a review of all content contained on information sharing portals[7] hosted on classified computer networks to identify particularly sensitive information[4] that should not be shared with the full user population able to access it. Reports and other content containing particularly sensitive information shall be securely removed as soon as possible, or access otherwise terminated, until appropriate access control regimes are in place to strictly limit readership to those with a need to know. The respective Chief Security Officer shall be notified when such content is identified for spill determination and response.	All Recipient D/As	9/30/2014
B-3. DNI will evaluate the sufficiency of existing policy guidance (e.g., ICDs 203, 209) and promulgate new or revised directives as necessary to protect intelligence sources, methods, and activities in written intelligence reports. The new or revised directives will be accompanied by guidance to include timetables for implementation by specified departments and agencies. In this process, DNI shall consider the following:	DNI All Recipient D/As (Upon promul-gation of guidance)	6/30/2014 12/31/2014

• Compose classified reports for maximum, yet safest utility and include particularly sensitive information[4] only when necessary. • Provide less sensitive versions of documents for wider audiences (e.g., tear lines) that include only essential data. • Avoid aggregating particularly sensitive information into a single document without controls limiting access commensurate with the sensitivity of the data (e.g., a graphic illustrating or enumerating global or cross-cutting capabilities). • Use pseudonyms or code words for particularly sensitive operational identities, locations, and technical parameters (e.g., source and partner identities, meeting and sensor locations, or technical parameters for weapons systems and military operations). • Create and enforce tiered levels of information sensitivity (e.g., level of detail about a program or capability controlled by need to know) to protect explicit or aggregated descriptions of particularly sensitive information. • Review, update, amend, or write classification guides for shared content restrictions to include the need to know principle. Upon completion of DNI's review and promulgation of guidance, the Senior Information Sharing and Safeguarding Steering Committee shall consider its applicability to non-Title 10/Title 50 departments and agencies and further task as appropriate.		

[7] This includes portals such as Wikis and SharePoint sites but excludes enterprise case management systems with native capability to restrict access based on need to know.
[8] The terms "enterprise audit" and "audit data" are used as defined in ICS 500-27 and the *Intelligence Community Enterprise Audit Conceptual Framework*.

Task Group C: Lockdowns and Automations for Privileged Functions		
Task	*Responsible Entity*	*Suspense*
C-1. Conduct a review of all privileged user roles and minimize their number, scope of privilege[9] ("least privilege"), and breadth of privilege (separation of duties). Separate roles for network or database administration from other sensitive functions, such as	All Recipient D/As	9/30/2014

cryptographic key management, hardware management, cross domain and removable media data transfer, system security management, or access to particularly sensitive information.[4]		
C-2. Institute separate administrator user accounts that tailor privileged access for particular users to the specific tasks at hand, such as those identified in task C-1.	All Recipient D/As	9/30/2014
C-3. Increase separation of duties and the application of "least privilege" through automation of systems administration, use of two-stage controls, and other means to reduce the need for privileged users or for such users to exercise their privileges in manual ways.	All Recipient D/As	12/31/2014
C-4. Ensure audit data[8] relating to the actions of privileged users are stored beyond the reach of those users and that all accesses to the data are also audited. Consolidate audit data to facilitate review.	All Recipient D/As	12/31/2014
C-5. Establish an ongoing practice that insider threat program personnel analyze audit data relating to the actions of privileged users. In the event a department or agency has yet to stand up its insider threat program hub, it should temporarily make use of an independent audit group to conduct the reviews.	All Recipient D/As	12/31/2014
[9] Adhere to the NCIX's Privileged User Working Group taxonomy and guidance.		

Task Group D: Reduce Removable Media Usage		
Task	*Responsible Entity*	*Suspense*
D-1. Implement two-stage controls for all transfers of data[10] from a classified computer network to removable media or to a network of lower classification.	All Recipient D/As	12/31/2014
D-2. Ensure enterprise audit is applied to all cross domain transfers and use of removable storage devices.	All Recipient D/As	6/30/2014
[10] Transfers of data from a classified computer network to removable media require the review and concurrence of a second person if not part of an approved internal use process, such as encrypted backups. Transfers of data to a network of lower classification through a supervised network gateway may involve an automated review stage coupled with human review. Such transfers may be completely automated in limited and suitably approved circumstances, such as the automated dissemination of tearline reporting. In circumstances when two-stage controls are not practicable, other risk mitigation measures must be applied.		

Task Group E: Control Access to Hardware Layers		
Task	*Responsible Entity*	*Suspense*
E-1. Review and improve protections for enterprise computing and communications equipment through procurement safeguards, physical security (single-person access to particularly sensitive locations must be avoided), and oversight of configuration changes.	All Recipient D/As	12/31/2014