EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

January 3, 2011

M-11-08

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Jacob J. Lew
Director

SUBJECT: Initial Assessments of Safeguarding and Counterintelligence Postures for Classified National Security Information in Automated Systems

On November 28, 2010, departments and agencies that handle classified national security information were directed to establish assessment teams to review their implementation of safeguarding procedures. (Office of Management and Budget, Memorandum M-11-06, "WikiLeaks - Mishandling of Classified Information," November 28, 2010.) These assessments were intended to build upon the existing requirement in Executive Order 13526 ("Classified National Security Information") for departments and agencies to establish and maintain ongoing self-inspection programs, in furtherance of the Executive Branch's comprehensive and enduring effort to strengthen our safeguarding and counterintelligence postures to enhance the protection of classified national security information.

Please see the attached memorandum from the Director of the Information Security Oversight Office (ISOO) and the National Counterintelligence Executive within the Office of the Director of National Intelligence (ODNI). Their offices will – consistent with their respective responsibilities under Executive Order 13526 and Section 1102 of the National Security Act of 1947 (as amended), and in coordination with the Office of Management and Budget – evaluate and assist agencies to comply with the assessment requirement and provide assistance to agency assessment teams. Their support will include periodic on-site reviews of agency compliance where appropriate. The attached memorandum calls for agency teams to complete their internal assessments by January 28, 2011.

Thank you for your cooperation and compliance with the further directions attached to this memorandum.

Attachment

MEMORANDUM FOR: Senior Agency Officials Designated Under Section 5.4(d) of Executive Order 13526, "Classified National Security Information"

FROM: Robert M. Bryant
National Counterintelligence Executive

William J. Bosanko
Director, Information Security Oversight Office

SUBJECT: Initial Assessments Pursuant to Office of Management and Budget Memorandum (M-11-06), "WikiLeaks – Mishandling of Classified Information," November 28, 2010

REFERENCES:

A. Office of Management and Budget Memorandum, "Initial Assessments of Safeguarding and Counterintelligence Postures for Classified National Security Information in Automated Systems," This Date
B. Executive Order 13526, "*Classified National Security Information*" (December 29, 2009)
C. Counterintelligence Enhancement Act of 2002, as amended

Strong counterintelligence and safeguarding postures are necessary to protect classified national security information. You have been charged with directing and administering the implementation of Executive Order 13526 ("Classified National Security Information") by the head of your department or agency. As such, you also have a significant role regarding compliance by your department or agency with the subject of this memorandum.

On November 28, 2010, the Office of Management and Budget directed departments and agencies that handle classified national security information to establish assessment teams (consisting of counterintelligence, security, and information assurance experts) to review their implementation of safeguarding procedures. In furtherance of that directive, please find attached a list of existing requirements and questions your department or agency assessment team should utilize, as an initial step, to assess the current state of your information systems security.

SUBJECT: Initial Assessments Pursuant to Office of Management and Budget Memorandum, "WikiLeaks – Mishandling of Classified Information," November 28, 2010

Each initial assessment should be completed by January 28, 2011, and should include the following with respect to the attached list of self-assessment questions:

1. Assess what your agency has done or plans to do to address any perceived vulnerabilities, weaknesses, or gaps on automated systems in the post-WikiLeaks environment.
2. Assess weakness or gaps with respect to the attached list of questions, and formulate plans to resolve the issues or to shift or acquire resources to address those weaknesses or gaps.
3. Assess your agency's plans for changes and upgrades to current classified networks, systems, applications, databases, websites, and online collaboration environments – as well as for all new classified networks, systems, applications, databases, websites or online collaboration environments that are in the planning, implementation, or testing phases – in terms of the completeness and projected effectiveness of all types of security controls called for by applicable law and guidance (including but limited to those issued by the National Security Staff, the Committee on National Security Systems, the National Institute for Standards and Technology).
4. Assess all security, counterintelligence, and information assurance policy and regulatory documents that have been established by and for your department or agency.

We look forward to working with you to implement this initial assessment and to ensure that your agency is best positioned to protect classified national security information. We will be in touch with agencies according to a prioritized, risk-based schedule in order to schedule a discussion of your initial assessments, as well as to arrange for subsequent onsite inspections, where appropriate.

We note that some agencies have also been asked to respond to an NCIX "Request for Information on Classified Networks and Systems" dated December 10, 2010, in support of National Security Staff tasking. We wish to distinguish that request from the requirements of this memorandum.

Robert M. Bryant

William J. Bosanko

Attachment:
As Stated

Initial Agency Self-Assessment Program for User Access to Classified Information in Automated Systems

Each department or agency that handles classified information should assess the agency's and its employees' adherence to the policy issuances noted below, the requirements to safeguard classified information *with an emphasis on their application in automated systems*, and any process the agency has designed to detect purposeful misuse of information technology systems. If your agency does not have any of the required programs/processes listed, you should establish them.

The initial Self Assessment items contained in this document pertain to security, counterintelligence, and information assurance disciplines, *with emphasis on their application in automated systems*. They are categorized as follows.

1) Management & Oversight
2) Counterintelligence
3) Safeguarding
4) Deter, Detect, and Defend Against Employee Unauthorized Disclosures
5) Information Assurance Measures
6) Education & Training
7) Personnel Security
8) Physical/Technical

Policy References – The initial Self Assessment items are drawn from various policy documents listed here.

1. EO 12968, Access to Classified Information
2. EO 13526, Classified National Security Information
3. 32 CFR 2001, Implementing Directive for EO 13526
4. Federal Information Security Management Act of 2002
5. EO 12333, United States Intelligence Activities
6. Counterintelligence and Security Enhancements Act of 1994
7. Counterintelligence Enhancement Act of 2002
8. National Security Presidential Directive (NSPD)-54/Homeland Security Presidential Directive (HSPD)-23, Cybersecurity Policy
9. Presidential Decision Directive/NSC-75, U.S. Counterintelligence Effectiveness: Counterintelligence for the 21st Century
10. Presidential Decision Directive/NSC-24, U.S. Counterintelligence Effectiveness
11. EO 13231, Critical Infrastructure Protection in the Information Age
12. Committee on National Security Systems Policy # 26, National Policy on Reducing the Risk of Removable Media
13. Committee on National Security Systems Policy #22, Information Assurance Risk Management Policy

14. Committee on National Security Systems Instruction #1253, Security Categorization and Control Selection for National Security Systems, dated October 2009
15. Section 1102 of National Security Act of 1947
16. National Security Directive – 42, National Policy for the Security of National Security Telecommunications and Information Systems

1. Management & Oversight:

- How does your agency ensure the self-inspection programs evaluate the adherence to the principles and requirements of the Executive Order 13526 (the Order) and 32 C.F.R. Part 2001 (the Directive) relative to safeguarding of classified information in automated systems?
  - Do required assessments cover the certification and accreditation of automated systems with respect to classified information?
  - Do required assessments cover safeguarding of classified information specific to automated systems?
  - Are corrective actions developed as indicated in the results/lessons-learned?
  - Are deficiencies tracked centrally to enable trend analysis?
  - Are security education and training programs updated to reflect common deficiencies and lessons learned?
  - Are agency policies reviewed regularly to address common deficiencies and lessons learned?
- Does your agency have sufficient measures in place to determine appropriate access for employees to classified information in au*tomated systems:*
  - *During initia*l account activation/setup?
  - Periodically to determine if access is adequate to perform the assigned tasks or exceeds those necessary to perform assigned tasks, and adjust them accordingly?
  - When IT audit *activities indicate* that employees are exceeding or attempting to exceed their permissions?
  - When IT audit activities indicate that removable media has been introduced and/or data is being written to removable media? and
  - When IT audit activities indicate that indicate preset thresholds have been exceeded or when employees "push" data over one-way transfer devices or when "data-mining" is indicated?
- How does your agency ensure that the performance contract or other system used to rate civilian or military personnel performance includes the designation and management of classified information as a critical element or item to be evaluated in the rating of all personnel whose duties significantly involve the creation or handling of classified information?
- Do supervisors evaluate employee's acceptance and adherence to the security rules for physical security, counterintelligence (CI), information assurance (IA), and overall information protection? Does this evaluation consider the issues specific to the use of automated systems?

2. Counterintelligence

- Does your agency have a counterintelligence program? If so:
  - Describe its mission and functions.
  - At what level is it funded annually?
  - Are the CI program personnel graduates of a counterintelligence training program for CI professionals at an Intelligence Community (IC)-based training entity? If not, when are they scheduled to attend?
  - Does the CI program interface with the information assurance element of your agency?
  - To what extent are anomalies that are discovered through your agency's information assurance processes brought to the attention of counterintelligence personnel? To what extent has this occurred over the past twelve months?
- Has your agency identified its high value information and processes that must be protected? What process is in place to update and reevaluate these?
- Describe what, if any, process your agency employs to regularly receive information to identify which of your agency's information or processes are of priority interest to adversary collectors?
- Does your agency have a process in place to evaluate its contracts, acquisitions, and procurements for foreign interest or involvement? If so, please describe the workings of that process.

3. Safeguarding:

- How does your agency ensure access to classified information in automated systems is limited to those persons who: (a) have received a favorable determination of eligibility from the agency head or their designee,(b) have signed an approved non-disclosure agreement, and (c) have a need to know the information?
- How does your agency ensure that procedures are in place to prevent classified information in removable media and other media (back-up tapes, etc.) is not removed from official premises without proper authorization?
- How does your agency employ procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information: (a) prevent access by unauthorized persons; and (b) ensure the integrity of the information?
- How does your agency employ controls to ensure classified information in an automated systems environment is used, processed, stored, reproduced, transmitted, and destroyed (removable and other media such as obsolete drives or back-up tapes) under conditions that provide adequate protection and prevent access by unauthorized persons and which assure that access to classified information is provided only to

authorized persons, and that the control measures are appropriate to the environment in which the access will occur and the nature and volume of the information?

- How does your agency ensure that persons who transmit removable and other media (back-up tapes, etc.) or who use automated systems to transmit classified information are held responsible for ensuring that intended recipients are authorized persons with the capability to store classified information?
- How does your agency ensure that classified information transmitted and received via automated systems or media is accomplished in a manner which precludes unauthorized access, provides for inspection for evidence of tampering and confirmation of contents, and ensures timely acknowledgment of the receipt by an authorized recipient?
- How are need-to-know determinations made in your agency reflected in your management of automated systems?
- Is classified information that is electronically accessed, processed, stored or transmitted via automated systems protected in accordance with applicable national policy issuances identified in the Committee on National Security Systems (CNSS) guidance and ICD 503, IC Information Technology Systems Security Risk management, Certification, and Accreditation?
- Do you employ alternative measures to protect against loss or unauthorized disclosure specific to automated systems?
- Does your agency allow the "modified handling and transmission" of foreign government information via automated systems? If so, how do you ensure sufficient safeguarding by using transmission methods approved for classified information, unless the method is waived by the originating government?
- How do you ensure that electronic and removable media are properly marked when they contain classified information? Do your risk management strategies consider the use of means to identify electronic media that contain classified information?
- How do you ensure that classified information is properly marked when used in the electronic environment?
- Do you control media access devices and ports on your IT systems to prevent data exfiltration?
- Have you instituted management measures to thwart deliberate bypass or circumventing the rules?
- Does your department or agency have a system to ensure that badges, clearances, and accesses are terminated when an employee no longer requires access?

4. Deter, Detect, Defend Against Employee Unauthorized Disclosures:

- Do you have an insider threat program or the foundation for such a program?
- Are there efforts to fuse together disparate data sources such as personnel security and evaluation, polygraph, where applicable, IT auditing or user activities, and foreign contact/foreign travel information to provide analysts early warning indicators of insider threats?
- Is there a collaborative effort between CI, IA, security, Inspector General (IG), Office of General Counsel (OGC), and Human Resources (HR)? Are these established through formal agreements, processes and procedures, and/or policies?
- What if anything have you implemented to detect behavioral changes in cleared employees who do not have access to automated systems?
- Are you practicing "security sentinel" or "co-pilot" policing practices?
- What metrics do you use to measure "trustworthiness" without alienating employees?
- Do you use psychiatrist and sociologist to measure:
    - Relative happiness as a means to gauge trustworthiness?
    - Despondence and grumpiness as a means to gauge waning trustworthiness?

5. Information Assurance Measures:

Specific to national security systems (NSS) that process classified information:

- How do you employ CNSS Policies, Issuances, Instruction, and Advisory Memorandums to certify and accredit your systems?
- Do you perform Risk assessments and security categorizations in accordance with CNSS, NIST and FIPS standards?
- What steps has your agency taken to implement the latest version of the NIST SP-800 series guidance on Information Assurance, Risk Management, and Continuous Monitoring?
- Do you employ NSA and FIPS encryptions to protect classified data in motion and data at rest?
- Do you collaborate with IA security (ISSM and ISSO) for:
    - trends indicating misuse/abuse,
    - a list of Privileged Users (PU) who have administrative access to systems and networks, and
    - a list of PU and General Users who have media-access (read/write/removable media port) privileges?
- How does your agency examine NSS and evaluate their vulnerability to foreign interception and exploitation?
- How do you assess the overall security posture of systems and disseminate information on threats to and vulnerabilities?

- Does your agency review, at least annually, existing risk management processes to ensure compliance with CNSS policy?
- What steps does your agency take to ensure risk assessments are conducted from an enterprise perspective, conducting top down assessments and analyzing the compilation of risks by individual information system owners?
- Does your agency require a formal enterprise-level Plan of Actions and Milestones (POA&M) containing (i) systemic information systems and organizational security weaknesses and deficiencies; (ii) risks relating to the identified weaknesses and deficiencies requiring further mitigation; (iii) specific actions to mitigate identified risks?
- What criteria has your agency established—and how are they enforced—for using removable media with your NSS? If your agency permits the use of removable media, what safeguards are employed and how are they promulgated and trained? How are you complying with CNSSP-26?
- If your agency permits the use of removable media:
    - How does your agency evaluate the effectiveness for implementing its policy on the use of removable media in national security systems?
    - Does your agency share lessons learned and best practices with respect to its use of removable media? What actions does your agency undertake to ensure that resources are available to implement its removable media policy; incorporating the content of removable media policy into user training and awareness programs; publishing and implementing incident response procedures.
    - How has it limited the use of removable media on NSS to those operational environments that require these media to achieve mission success and not simply for convenience?
    - What efforts has your agency undertaken to avoid the use of removable media by making maximum use of properly configured and secured network shares, web portals, or cross domain solutions to transfer data from one location to another?
    - What risk management policies has your agency crafted, promulgated, and implemented to reduce risks to NSS? How do you verify their implementation?
    - Does the agency restrict use to removable media that are USG-owned and that have been purchased or acquired from authorized and trusted sources?
    - Does the agency scan removable media for malicious software using a department or agency-approved method before introducing the media into any operational systems?
    - Does the agency prohibit automatic execution of any content by removable media unless specifically authorized by the Chief Info Security Officer? Are spot checks conducted or how is compliance verified?
    - Does the agency implement access controls (e.g., read/write protections) for removable media? How are those controls implemented?
    - Does the agency encrypt data on removable media using, as a minimum, the Federal Information Processing Standard (FIPS) 140-2?

- Does the agency prohibit use of removable media for data transfer from the destination network back to the source network or to any other network unless the media have been erased, reformatted, and rescanned? How do you verify this?
- Does your agency limit the use of removable media to authorized personnel with appropriate training? What training is conducted? When? How is the adequacy of training evaluated?
- Does your agency implement a program to track, account for, and safeguard all acquired removable media, as well as to track and audit all data transfers? How are discrepancies handled? What discrepancies have occurred within CY 2010?
- Does your agency conduct both scheduled and random inspections to ensure compliance with department/agency-promulgated guidance regarding the use of removable media? What is the frequency? What are the results?
- Does your agency sanitize, destroy, and/or dispose of removable media that have been used in National Security Systems (NSS) in accordance with a department or agency-approved method, when the media are no longer required? What double-check or verification procedures exist?

6. Education and Training:

- How does your agency ensure that every person who has access to classified information via automated systems has received contemporaneous training on the safeguarding of classified information?
- How does your agency implement security education and training program(s) that ensure employees who create, process, or handle classified information in automated systems have a satisfactory knowledge and understanding of safeguarding policies and procedures specific to automated systems?
- What initial, refresher, or specialized training is provided to your personnel specific to automated systems and appropriate to their duties and responsibilities?
- What are the methods of delivery your organization uses to provide education, training and awareness programs for CI, and IA to users of automated systems? (New hire orientation, semi-annual/annual courses, computer based training?)
- Is CI, security, information security, information systems security, social networking, incident and/or suspicious activity reporting all covered?
- How does your agency ensure that persons who have access to classified information understand their responsibility to report any actual or possible compromise or disclosure of classified information to an unauthorized person(s) to an official designated for this purpose?
- Are users of automated systems made aware of confirmed violations of the stated security policy and the ramifications of those actions, in order to demonstrate the organization's commitment to its security policies?

- Does your training address "need to know" decisions specific to automated systems?
- Does your training include the penalties for providing false or incomplete information to security investigators during background checks or special security investigations?
- What organizations within your agency manage the security education and training programs for users of automated systems (CI, Security, IA)? Is the training separate, or combined into an integrated, comprehensive and structured CI, Security and IA program?
- Are CI, Security and IA training materials current, and consolidated into a single electronic site for ease of reference?
- Are Rules of Behavior/ Acceptable Use agreements signed by individuals (before they are given facility and network access) that acknowledge they understand the information that was presented to them during the training? Are the ramifications for violations of security policies and procedures discussed?
- In addition to General User Acceptable Use Agreements referenced above, are Privileged User Roles and Responsibilities Acknowledgment Agreements signed. (Privileged User: Network Administrators, Network Security Engineers, Database Administrators, Software Developers, etc.)
- Have you instituted an "insider threat" detection awareness education and training program, and if so, how has it affected employee performance or participation in security programs?
- How do you follow CNSSD-500 & CNSSI 4000 series with regard to IA Education and awareness training for:
    - Infosec professionals
    - Senior System Managers
    - Systems administrators,
    - ISSO's
    - Systems Certifiers, and
    - Risk Analysts?
- How do you ensure personnel are informed of CNSS Advisory Memorandums regarding:
    - Insider Threats to USG Information Systems
    - Web Browser Security Vulnerabilities
    - Firewall & Guard protection methods?
    - The IA Approach to Incident Management?

7. Personnel Security:

- Have you established a comprehensive personnel security program? If so, please describe your investigative, adjudicative, and continuous evaluation processes. Do you train your adjudicators to look for insider threat indicators?
- Have you conducted a trend analysis of indicators and activities of the employee population which may indicate risky habits or cultural and societal differences other

than those expected for candidates (to include current employees) for security clearances?

- Do you have a foreign travel/contacts reporting process or system that identifies unusually high occurrences of foreign travel, contacts, or foreign preference in the investigative subject pool?
    - Does your CI organization have access to the information?
    - Do you have mandatory pre-and post-travel briefings for government and contractors?
    - Does your agency have a program to control foreign visitors?
    - Do you require reporting of official and non-official travel/contacts?
    - Under what circumstances are employees not required to report foreign contacts?
    - If you don't have a foreign travel reporting process, do you plan to establish one? What is the timeframe?
    - Do you capture higher than usual occurrence of unauthorized disclosures or security violations?
    - Do you track circumstances whereby certain employee candidates have applied to multiple departments or agencies seeking employment with access to classified information?
    - Do you capture evidence of pre-employment and/or post-employment activities or participation in on-line media data mining sites like WikiLeaks or Open Leaks?
- Do you receive regularly updated threat and vulnerability reports that support:
    - Your risk management decisions,
    - Your training and educations program, and
    - Your personnel and physical/technical security programs?
- Do you collaborate among the counterintelligence, personnel security and polygraph programs for indications of CI activities (both targeted at your agency and from within)?
    - Do you have access to:
        - ✓ Facility and IA certification and accreditation reports, and
        - ✓ Facility and IA Plans of Action and Milestones (POA&Ms) for resolving known/identified deficiencies?
- How and to what extent does your agency interface with the FBI of foreign intelligence concerns? Is your agency familiar with reporting requirements to the FBI under section 811 of the Counterintelligence and Security Act of 1994? Has your agency field an 811 report to the FBI in the previous twelve months?
    - Is your department or agency familiar with the Department of Justice CES requirements relative to media leaks?
    - Are you conducting liaison with internal and external investigative activities related to employee security or suitability issues?
        - ✓ Monitoring FBI investigations subsequent to 811 referrals, and
        - ✓ OPM for debarment/removal actions of employees subsequent to wrongful acts?
- Are all employees required to report their contacts with the media?

8. Physical/Technical Security:

- Has your agency developed annual reports of the status and welfare of the secure facilities that support the protection of classified information and mission accomplishment?
- Has your agency conducted a trend analysis for activities and events affecting information protection at any particular site or a group of sites?
- Do you look for unscheduled maintenance or unusual failures of security hardware (which might indicate end-of-life deficiencies or insider manipulation)?
- Are Technical Surveillance Countermeasures employed in areas where sensitive information is discussed?