

TESTIMONY OF JOHN FITZPATRICK
DIRECTOR OF THE INFORMATION SECURITY OVERSIGHT OFFICE
BEFORE THE
HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT OPERATIONS
ON

***“PSEUDO-CLASSIFICATION OF EXECUTIVE BRANCH DOCUMENTS: PROBLEMS
WITH THE TRANSPORTATION SECURITY ADMINISTRATION’S USE OF THE
SENSITIVE SECURITY INFORMATION DESIGNATION”***

MAY 29, 2014

Chairman Mica, Ranking Member Connolly, and members of the Subcommittee, thank you for inviting me to testify before you today. I am John Fitzpatrick, the Director of the Information Security Oversight Office (ISOO) at the National Archives and Records Administration (NARA). ISOO is responsible to the President for policy and oversight of the government-wide security classification system, the National Industrial Security Program, the Classified National Security Information Program for State, Local, Tribal, and Private Sector entities, and the Controlled Unclassified Information (CUI) Program. ISOO’s mission is to ensure the government protects and provides proper access to information to advance the national and public interest. We accomplish this by leading efforts to standardize and assess the management of classified information and CUI through oversight of department and agency practices, policy development, guidance, education, and training.

In my testimony, I will focus on the CUI Program’s core policy objectives and current state of development.

The CUI Program is designed to reform a fundamental problem in the Executive branch of an inefficient, confusing patchwork of *ad hoc* agency-specific policies, procedures, and

markings. These agency-specific policies are sometimes unclear to the public and result in inconsistent marking and safeguarding of documents, uncertain dissemination policies, and impediments to authorized information sharing.

President Bush identified the need for a uniform policy, which led to the May 2008 Memorandum¹ that charged NARA as Executive Agent to create a program centered on standardizing the handling of terrorism-related information within the Information Sharing Environment. In turn, the Archivist of the United States established a CUI Office to accomplish this task. On May 27, 2009, President Obama established a CUI Task Force², chaired by the Departments of Homeland Security and Justice to review Sensitive but Unclassified (SBU) information practices and make recommendations on implementing a comprehensive CUI policy. On December 15, 2009, Secretary Janet Napolitano and Attorney General Eric Holder jointly released the *Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information*, which included a specific recommendation for expansion of the CUI policies beyond the original terrorism-related information scope.³

On November 4, 2010, President Obama signed Executive Order 13556 “Controlled Unclassified Information”⁴ (the Order), establishing a CUI Program to reform the way in which the Executive branch handles its sensitive information by establishing one uniform system to help agencies manage all unclassified information that requires safeguarding and/or

¹ Presidential Memorandum for the Heads of Executive Departments and Agencies on “Designation and Sharing of Controlled Unclassified Information (CUI),” May 07, 2008.

² Presidential Memorandum for the Heads of Executive Departments and Agencies on “Classified Information and Controlled Unclassified Information,” May 27, 2009.

³ <http://www.dhs.gov/news/2009/12/15/presidential-task-force-controlled-unclassified-information-releases-report-and>

⁴ Executive Order 13556 “Controlled Unclassified Information,” November 04, 2010.

dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies. The Order rescinded the May 2008 terrorism-related memorandum and identifies NARA as the Executive Agent to implement the program and oversee department and agency actions to ensure compliance. The Archivist of the United States subsequently tasked ISOO with this mission.

One of the program's core policy objectives is to promote openness and transparency. The CUI Program will replace the current patchwork of agency-specific practices with a single, open and uniform system of policies, procedures, and markings. In addition to helping agencies protect sensitive information, this new framework is intended to remove impediments to authorized information sharing through increased clarity and consistency of practice. Open and clear guidance is expected to enhance trust among agencies and result in increased information sharing. Transparency of these practices should increase the confidence of the American public in the new CUI Program.

We maintain a publicly available CUI Registry of all categories and subcategories of information that meet the Executive Order's standard for protection, namely, the requirement that law, Federal regulation, and government-wide policy require control of the information. Following issuance of the Order, Executive branch agencies reviewed their respective SBU information practices and submitted to the Executive Agent those categories and subcategories that they wished to continue to employ. ISOO reviewed more than 2,200 category and subcategory submissions from 47 agencies and led interagency discussions to consolidate redundancies, provide consistency among like categories and subcategories, and ensure consistency with the standards of the Order. To minimize unnecessary control, the Executive Agent rigorously applied the requirement of the Executive Order that "if there is significant

doubt about whether information meets the standard for CUI, it shall not be so designated as such.”⁵

The authorized categories and subcategories of CUI are defined in the CUI Registry along with hyperlinks to authorizing laws, regulations, and government-wide policies that establish the basis for the control of the information. There are currently 22 categories and 85 subcategories of such information, ranging from sensitive nuclear and critical infrastructure information, to personal privacy and business proprietary data, as well as a host of other information types.

Sensitive Security Information (SSI) is one such subcategory and is properly authorized to be controlled on the basis of 49 USC 114 (r), 49 CFR 1520, 49 USC 40119(b)(1), and 49 CFR 15. Under the CUI Program, the specific statutory and regulatory requirements for SSI, such as the safeguarding, dissemination, and disposal of the information will stay the same, while global CUI marking requirements for SSI will be implemented.

Under the CUI Program, the CUI Registry will also contain all policies and guidance for the proper marking and handling of CUI, once these are finalized. This serves to enhance openness and transparency by making the government basis for establishing information controls available for all to see. These policies and procedures have been developed in consultation with the CUI Advisory Council, an interagency body established in June 2013 to advise the CUI Executive Agent on the development and issuance of policy and implementation guidance for the CUI Program. The Council is chaired by the Director of ISOO, and current membership is based on that of the Chief Financial Officers’ Council with representatives from 28 agencies to include the Departments of Transportation and Homeland Security, who are regular participants. We

⁵ Section 3(b).

also actively seek feedback from State, local, tribal, private sector, as well as public interest groups. ISOO has met with public interest groups throughout the policy development process and incorporated their comments and suggestions.

With formal input from the Council, Council-nominated subject matter experts, and other stakeholders (both Federal and non-Federal), policy has been developed concurrently on multiple levels:

1. An implementing directive to be incorporated into the Code of Federal Regulations (CFR) will include principles and guidelines of the CUI Program applicable to all information and Executive branch users with a lawful government purpose;
2. Supplemental Guidance, including, but not limited to, more detailed procedures, definitions and protocols for appropriate safeguarding, dissemination, marking and decontrol of unclassified information; and,
3. Expansion of the CUI Registry to reflect any additional authorized categories and subcategories, markings, designation authorities, specified CUI requirements, and a glossary of terms.

The draft regulation is currently being reviewed by other Executive Branch agencies and ISOO will collect and respond to their comments. After the inter-agency review process, ISOO will proceed with the balance of the federal rule making process.

The relationship between the CUI Program and the Freedom of Information Act (FOIA) provides further evidence that openness and transparency are desired outcomes of the CUI Program. Executive Order 13556 draws a bright line between the two, emphasizing that “the mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter

of discretion.”⁶ Decisions to disclose or withhold information must be made solely based on the applicability of the statutory exemptions contained in the FOIA (or other applicable laws, regulations, or policies) and at the time of a request for information.

In short, CUI markings and status should not serve as a basis to improperly withhold or improperly disclose information from or to the public, including under the FOIA. This point has been clarified in guidance we jointly issued with the Department of Justice’s Office of Information Policy.⁷ In addition, we developed publicly available on-line training based on the joint guidance to educate and provide additional clarity.⁸

Another core objective of the CUI program is strong accountability and oversight. The first step toward meeting this objective entails requiring Executive branch agencies to appoint a senior agency official and a program manager responsible to their agency head, and ISOO, for program implementation within that agency, which ISOO required through its April 11, 2013 memorandum to the agency heads.⁹ These designated officials are responsible for drafting agency implementing policies, training their employees on program requirements, implementing new practices while phasing out old ones, and establishing a robust self-inspection program to ensure ongoing compliance.

In consultation with the CUI Advisory Council and OMB, consistent with the Executive Order¹⁰ the Executive Agent is looking to establish deadlines for phased implementation for the

⁶ Section 2(b).

⁷ “Guidance regarding Controlled Unclassified Information and the Freedom of Information Act”, November 22, 2011.

⁸ <http://www.archives.gov/cui/training.html>

⁹ “Appointments of Senior Agency Official and Program Manager for Controlled Unclassified Information (CUI) Program Implementation,” April 11, 2013.

¹⁰ Section 5(b).

Executive branch that will be set forth in a National Implementation Plan. Implementation will begin with the publication of the final regulation in the CFR and the issuance of the supplemental guidance. ISOO expects that agencies will require about one year after publication of the final regulation to reach initial operating capability, by preparing their internal implementing policies based on the national guidance and conducting their training of employees to handle, recognize, and receive CUI. We plan to assist these efforts by providing online basic CUI training that will be published on ISOO's website. It is anticipated that based on budgetary cycles and the required transition of information systems, the elimination of old SBU markings and their replacement by the new CUI standards, procedures, and markings will take place within two to three years after initial operating capability is reached.

ISOO will oversee these agency actions in multiple ways, including reviewing agency policies, conducting on-site inspections, and requiring agencies to periodically report on the program's status. We are also required under the Executive Order to regularly publish a report to the President on the status of agency implementation. These reports are made public along with ISOO's other reports on the status of the classification system. Taken together, these requirements will help ensure this program is properly and successfully implemented.

In conclusion, ISOO has established a reputation in the government for effective, objective oversight, consistency in practice, and maintenance of mature, constructive relationships with our agency partners. We are well on our way to establishing a stable and robust CUI Program, effectively integrating CUI into ISOO's Executive branch-wide role. Thank you very much for your time and the opportunity to appear before you today. I will be happy to answer your questions.