The White House

Office of the Press Secretary

For Immediate Release
October 07, 2011

Fact Sheet: Safeguarding the U.S. Government's Classified Information and Networks

Following the unlawful disclosure of classified information by WikiLeaks in the summer of 2010, the National Security Staff formed an interagency committee to review the policies and practices surrounding the handling of classified information, and to recommend government-wide actions to reduce the risk of a future breach. Since then, this effort has been a top priority of the Administration and senior agency officials have been actively engaged in developing policies and oversight mechanisms to enhance our national security through responsible sharing and safeguarding of classified information.

The strategic imperative of our efforts has been to ensure that we provide adequate protections to our classified information while at the same time sharing the information with all who reasonably need it to do their jobs. The guiding principles during the Administration's review were to:

- Reinforce the importance of responsible information sharing and not undo all of the significant and important progress we've made in interagency information sharing since 9/11;
- Ensure that policies, processes, technical security solutions, oversight, and organizational cultures evolve to match our information sharing and safeguarding requirements;
- Emphasize that effective and consistent guidance and implementation must be coordinated across the entire Federal government. We are only as strong as our weakest link and this is a shared risk with shared responsibility; and;
- Continue to respect the privacy, civil rights, and civil liberties of the American people.

The committee that was established in the wake of WikiLeaks proposed a new oversight structure to orchestrate the development and implementation of policies and standards for the sharing and safeguarding of classified information on computer networks. These structural reforms are reflected in the Executive Order signed today by President Obama.

In accordance with today's Executive Order:

- **Agencies bear the primary responsibility** for sharing and safeguarding classified information, consistent with appropriate protections for privacy and civil liberties. Federal agencies that use classified networks will:
    - designate a senior official to oversee classified information sharing and safeguarding for the agency;
    - implement an insider threat detection and prevention program; and
    - perform self assessments of compliance with policy and standards.
- A **Senior Information Sharing and Safeguarding Steering Committee** will have overall responsibility for fully coordinating interagency efforts and ensuring that Departments and Agencies are held accountable for implementation of information sharing and safeguarding policy and standards.
- A **Classified Information Sharing and Safeguarding Office** will be created within the office of the Program Manager for the Information Sharing Environment to provide sustained, full-time focus on sharing and safeguarding of classified national security information. The office will also consult partners to ensure the consistency of policies and standards and seek to identify the next potential problem.
- Senior representatives of the Department of Defense and the National Security Agency will jointly act as the **Executive Agent for Safeguarding Classified Information on Computer Networks** to develop technical safeguarding policies and standards and conduct assessments of compliance.
- An **Insider Threat Task Force** will develop a government-wide program for insider threat detection and prevention to improve protection and reduce potential vulnerabilities of classified information from exploitation, compromise or other unauthorized disclosure.

We did not, however, wait for today's Executive Order to begin taking steps. The Senior Information Sharing and Safeguarding Steering Committee formally established today began meeting informally in June to track steps taken across the Federal Government. In addition to those measures identified in today's Executive Order, significant progress has been made by U.S. Departments and Agencies in five priority areas:

1. **Removable media**

Departments and Agencies have made significant progress in clarifying and standardizing removable media policies, processes, and technical controls. We have limited the numbers of users with removable media permissions and strengthened accountability for violations.

2. **Online Identity Management**

The owners and operators of classified systems are accelerating efforts to strengthen the online verification of individuals logging on to classified systems, and to be able to track what information is being accessed by these individuals.

3. **Insider Threat Program**

As directed in the Executive Order, the Attorney General and the Director of National Intelligence are actively establishing an interagency Insider Threat Task

Force. This Task Force will integrate specialized abilities, tools, and techniques to more effectively deter, detect, and disrupt the insider threat.

4. **Access control**

Departments and Agencies are implementing more robust access control systems to enforce role-based access privileges that serve to ensure that an individual user's information access is commensurate with his/her assigned role.

5. **Enterprise audit**

Enhancing auditing capabilities across U.S. Government classified networks is a priority effort, and planning has been initiated to define the policy and develop standards for the collection and sharing of audit and insider threat data.