

Improving Protection While Expanding Access

- [State, Local, Tribal and Private Sector Partners Security Framework](#)
- [Information Systems Security](#)
- [Identity and Access Management](#)
- [Updated Policy for Handling Classified Information](#)
- [Expanding Discovery and Access in the Intelligence Community](#)

Information Systems Security

Reciprocity of IT system security certification and the acceptance and recognition among participating ISE agencies of each other's accreditation decisions is another important factor in ensuring efficient and effective information sharing. Several initiatives - led jointly by NIST, the Committee on National Security Systems (CNSS), and the ODNI - have made considerable progress in updating and harmonizing federal security standards and processes, setting the stage for future extensibility to state, local, tribal, and private sector partners.

With the issuance of NIST Special Publication 800-53 in August 2009 and CNSS Instruction 1253 in October 2009, the IC, DoD, and civilian federal agencies, for the first time, have adopted a common set of security controls that forms a de facto national baseline for all federal information systems. "Recommended Security Controls for Federal Information Systems and Organizations" are available on the [NIST website](#) ^[1] and "Security Categorization and Control Selection for National Security Systems" is available on the [Committee for National Security Systems](#) ^[2]. Alignment of these controls and further issuance of publications relating to risk management and security assessment will enhance interoperability among federal agencies. Although agency certifiers and accreditors will tailor requirements to their own environments, using the same standards will enable reciprocity ? agencies accepting each others? systems security testing ? when interconnecting systems.

The alignment and harmonization of federal information systems security standards on a common baseline will, in turn, present state, local, tribal, and private sector partners with a single, predictable security goal to meet. Harmonized standards will also enable implementation of reciprocity policies, not only among federal agencies and systems, but with state, local, tribal, and private sector partners as well, thereby reducing the time - and cost - required to interconnect systems.

Identity and Access Management

Properly identifying and authenticating users of IT systems is a necessary condition for trusted operations. The Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Part A, was developed by the Identity, Credential, and Access Management Subcommittee (co-chaired by the General Services Administration and DoD) of the Federal CIO Council in November 2009. This document provides a common segment architecture and associated implementation guidance for use by federal agencies as they continue to invest in FICAM programs. The FICAM segment architecture will

serve as an important tool for providing awareness to external mission partners and will drive the development and implementation of interoperable solutions. The [Global Federated Identity and Privilege Management \(GFIPM\)](#) [3] and the Trusted Broker systems are two approaches in use today that work toward interoperating under the FICAM umbrella.

When fully implemented, FICAM will close identified security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing. It supports the integration of physical access control with enterprise identity and access systems, and enables information sharing across systems and agencies with common access controls and policies. Leveraging the digital infrastructure in a secure manner will enable the transformation of business processes, many of which are vital to the security of the United States.

In addition to important progress in aligning access management procedures, PM-ISE sponsored groundbreaking work with NIST and DHS to develop an automated means to evaluate access management policies. Using new algorithms to electronically translate policies and regulations in natural language into automated instructions, NIST developed a pilot system that evaluates multiple policies, identifies gaps and contradictions, and reveals the actual access that results from overlaying more than one policy. As more and more information passes through many mission partners and systems, each with different access policies, the significance of automating access policies will be increasingly necessary to ensure efficient and appropriate access.

Updated Policy for Handling Classified Information

Improving protection and expanding access are complementary, not conflicting, goals. The policy governing the handling of classified national security information has undergone significant revision over the past year designed to ensure that classification is not a barrier to providing information to those who need it in a timely way. On December 29, 2009 - following a Presidentially-mandated 90-day review - the Administration released [Executive Order \(EO\) 13526](#) [4], which governs the handling, marking, and eventual declassification of Classified National Security Information. The new order replaces EO 12958, and provides more "accurate and accountable application of classification standards and routine, secure, and effective declassification".

Expanding Discovery and Access in the Intelligence Community

The Intelligence Community has continued the transformation of information sharing by implementing IC Directive (ICD) 501, "Discovery and Dissemination or Retrieval of Information." This policy promotes responsible information sharing by distinguishing between discovery (obtaining knowledge that information exists) and dissemination or retrieval (obtaining the contents of the information). The policy directs all IC elements to fulfill their "responsibility to provide" by making intelligence discoverable by automated means by authorized IC personnel. It also establishes procedures for gaining access to information that has been discovered and resolving disputes if access is denied.

Through the implementation of ICD 501, the IC has made considerable progress on improving information sharing by enabling discovery of disseminated analytic products through the creation of the Library of National Intelligence (LNI). LNI uses a combination of attribute-based access, tagged data, and auditing to promote secure information sharing of more than three million intelligence products.

Metadata tagging - information about other data - is crucial to ICD 501 implementation and is the linchpin

to the effective management of data throughout the intelligence cycle. It facilitates discovery, retrieval, and protection. The IC is using XML as the standard for metadata implementation, and most IC elements are meeting IC metadata standards required to submit products to the LNI.

The Value of the LNI

People with a mission need are increasingly able to conduct a single search of the IC's disseminated analytic products, covering 99% of the included product lines, compared to the past where users had to visit over 50 different websites to discover the same information.

The next steps include making the LNI more complete and timely while improving the quality of the metadata in the LNI, which will further improve the ability of users to search for disseminated analytic products as well as developing a secure repository for discovery of sensitive intelligence products by authorized IC personnel.

- Establishment of a National Declassification Center;
- Measures to address the problem of over-classification;
- Greater emphasis on sharing classified information among those who need it, including redefinition of the "need to know" principle and less restrictive rules for sharing classified information between agencies; and
- Provisions that ensure greater openness and transparency in the government's Classification and Declassification Programs.

Source URL: <http://www.ise.gov/improving-protection-while-expanding-access>

Links:

[1] http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[2] http://www.cnss.gov/Assets/pdf/Final_CNSSI_1253.pdf

[3] <http://gfipm.net/>

[4] <http://www.ise.gov/sites/default/files/EO13526.pdf>