Looking Forward

2015+ Federal Identity, Credential, and Access Management

A Key Driver

Home • Briefing Room • Presidential Actions • Executive Orders

The White House
Office of the Press Secretary

E-Mail Tweet Share +

For Immediate Release — October 17, 2014

Executive Order --Improving the Security of Consumer Financial Transactions

EXECUTIVE ORDER

- - - - - - -

IMPROVING THE SECURITY OF CONSUMER FINANCIAL TRANSACTIONS

Given that identity crimes, including credit, debit, and other payment card fraud, continue to be a risk to U.S. economic activity, and given the economic consequences of data breaches, the United States must take further action to enhance the security of data in the financial marketplace. While the U.S. Government's credit, debit, and other payment card programs
the security of consumer data
protects privacy and confiden

By the authority vested in me
order to improve the security
ordered as follows:

Section 1. Secure Governmen
doing business with the Gove
transition payment processing
features, including chip-and-P
consider relevant voluntary consensus standards and specifications, as appropriate, consistent with the National

Sec. 3. Securing Federal Transactions Online. To help ensure that sensitive data are shared only with the appropriate person or people, within 90 days of the date of this order, the National Security Council staff, the Office of Science and Technology Policy, and OMB shall present to the President a plan, consistent with the guidance set forth in the 2011 National Strategy for Trusted Identities in Cyberspace, to ensure that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate. Within 18 months of the date of this order, relevant agencies shall complete any required implementation steps set forth in the plan prepared pursuant to this section.

Executing the Vision

- **Identity, Credentialing, and Access Management** is the crux of cybersecurity: knowing who is accessing an agency's data/networks is critical to securing them.
- **Refine** the ICAM policy architecture to empower agencies to use risk-based decision-making to determine their respective desired states of ICAM maturity.
- **Facilitate** a procurement environment so agencies can acquire or update their ICAM capabilities.
- **Recognize** that we have unique requirements, but that we are not so special that what exists and has been done in the market can not be adopted in the Federal Enterprise
- **Engage** a broad set of stakeholders and roles to grow the federal ICAM community, including Mission Owners, CIOs, CISOs, implementers, CSOs, HR, etc. as well as state, industry, and citizens.
- **Align** the target state for ICAM with federal cybersecurity initiatives, such as the National Strategy for Trusted Identities in Cyberspace (NSTIC).
- **Foster** agencies' adoption of ICAM solutions, enabling compatibility across multiple domains, to include classified and unclassified.
- **Modernize** the collaborative environment for ICAM implementers, agency stakeholders, and industry to improve service delivery and breed innovative solutions, including shared services.

Beyond HSPD-12: PIV is an Enabler

Cybersecurity

Strengthens the security and resiliency of critical infrastructure against evolving threats to safeguard the government.

References:

- Cybersecurity Strategy
- FISMA
- PPD on Critical Infrastructure Security and Resilience

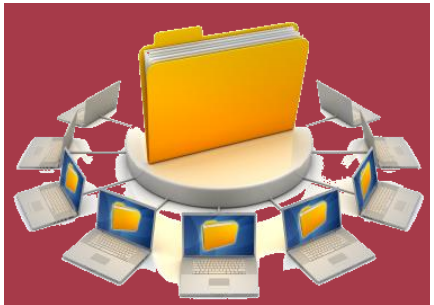
E-Government

Promotes the use of electronic forms and offers online-based government services for strong authentication.

References:

- The Digital Government Strategy
- E-SIGN Act
- E-Government Act

Information Sharing



Encourages sustained, responsible, and trusted collaboration to support interoperability across the government.

References:

- National Strategy for Information Sharing and Safeguarding
- ISS EO 13587

Good Steward of IT Resources

Emphasizes planning and spending control processes for investment in information systems to support agency missions.

References:

- Clinger-Cohen Act
- M-12-10: PortfolioStat
- M-13-02: Strategic Sourcing

4

Refining Metrics

Background

OMB is driving the shift from a compliance-based to value-based ICAM performance measurement system. This fundamental change in metrics would allow for an improved ability to measure and understand the security posture of the Federal Government. To facilitate this, various metrics related to ICAM will be streamlined and harmonized.

Objective

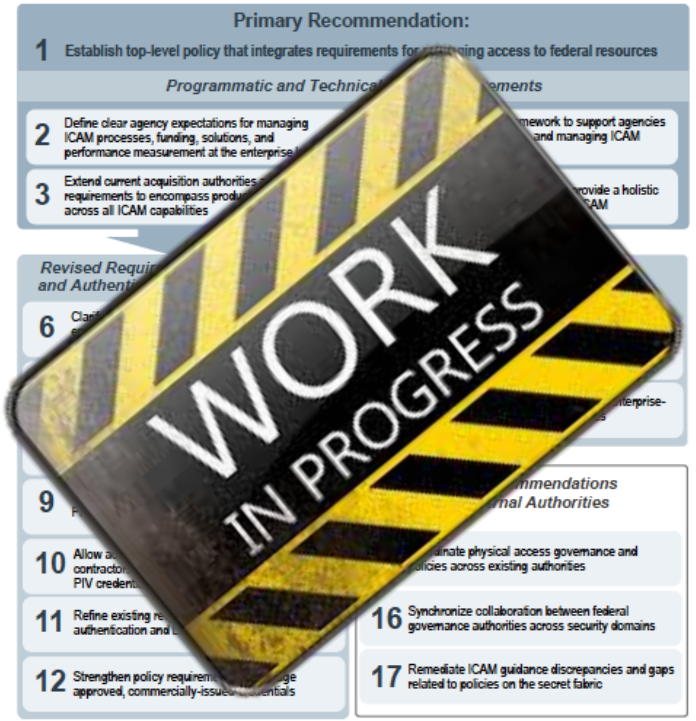
Revise FISMA metrics to reflect the updated policy direction, architecture, and harmonization of KISSI, CAP, and other reporting requirements. Metrics should leverage any available automated collection capabilities (e.g., CDM).

Policy, Standards, and Guidance

A Policy, Standards, and Guidance Tiger Team will deliver recommendations for revising ICAM standards based on identified gaps and propose a path forward to address these gaps through revised/new policy, standards, or guidance.

Establish a holistic approach that integrates requirements for managing access to federal resources

- Develop a granular framework for making risk-based decisions with regard to ICAM processes and solutions
- Foster an enterprise approach to ICAM management and clarify implementation expectations for agencies
- Consider new PIV/credential-related requirements to close gaps across user populations and address exceptional use cases
- Adjust risks and impacts per the Consumer Protection EO
- Coordinate with external authorities to improve governance and close gaps related to physical security and FICAM across security domains



Next Steps

ICAMSC leadership is working to develop a 24-month work plan to support the vision of the ICAMSC and shape the path forward for ICAM across the government.

FY15 Docket	
Docket Item	**Description**
 Policy and Standards Review and Recommendation	Deliver recommendations for revising ICAM standards based on identified gaps and propose a path forward to address these gaps through revised/new policy, standards, or guidance.
ICAM Architecture	Develop a revised ICAM architecture and enhance the ICAM service areas and use cases to align with the current environment.
 ICAM Playbook	Present ICAM content, including the ICAM service areas, use cases, and other relevant guidance and tools, via an interactive online interface.
 ICAM Metrics Architecture	Develop recommendations for ICAM metrics and rationalize existing ICAM data points with entities such as FISMA, KISSI, and PortfolioStat.
Revised ICAM Maturity Model	In alignment with the updated ICAM architecture and metrics, develop an agile, user-friendly maturity model to facilitate agencies' determination of maturity across the ICAM service areas to inform metric reporting and accountability.

Questions