

Information Security and Identity Management Committee (ISIMC) Charter

1. Purpose:

To provide a consensus based forum to support the Federal CIO Council (FCIOC) that enables Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) to collaborate on: (1) identifying high priority security and identity management initiatives; and (2) developing recommendations for policies, procedures, and standards to address those initiatives that enhance the security posture and protection afforded to Federal Government networks, information, and information systems.

2. Functions:

The Information Security and Identity Management Committee (ISIMC) shall be the principal interagency forum for identifying and recommending strategic high priority IT security and identity management initiatives to the FCIOC and OMB that enable Federal Government's information systems security programs and agencies' mission objectives through a comprehensive and consistently implemented set of risk-based, cost-effective controls and measures. The committee will recommend standard organization structures for information security committees across the Federal government; and ensure the tools, metrics and measures will lead to defensive operational capabilities and protections of the Federal networks, systems and applications. The Committee shall establish and oversee appropriate subcommittees, working groups, and/or task forces to perform the following functions:

- (A) Develop strategies to coordinate and facilitate the FCIOC's activities in support of the execution of the Comprehensive National Cybersecurity Initiative (CNCI) (National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23)), including:
 - (1) Presidential Strategies and Directives;
 - (2) secure computing platforms and networks; and
 - (3) agency alignment with United States Computer Emergency Readiness Team (US-CERT) incident response.

- (B) Identify and recommend information security and identity management enhancements to policies, processes, and solutions, that address the strategies in (A) above and improve upon identification management solutions, including:
 - (1) HSPD-12 logical access and integration with physical access and Public Key Infrastructure (PKI) practical applications/lessons learned in implementing user authentication;
 - (2) multi-factor authentication,
 - (3) device authentication/quarantine; and
 - (4) Federal bridging of credentials/certificates between agencies.

- (C) Provide oversight of the ISIMC subcommittees, working groups, and task forces. Coordinate with and provide advice to other Federal committees to improve collaboration, identify complimentary activities, and reduce duplication in security and identity management related areas. Review and concur on common security management requirements, performance measures, and Federal Enterprise Architecture (FEA) updates, program management plan, fiscal budget and funding strategy for security management service areas.

Information Security and Identity Management Committee (ISIMC) Charter

(D) Promote the development and use of standard performance measures for agency information security that:

- (1) Are outcome-based;
- (2) Focus on risk management;
- (3) Align with the business and program goals of the agency;
- (4) Measure improvements in the agency security posture over time;
- (5) Ensure collaborative Federal defensive security capabilities are prioritized; and
- (6) Reduce burdensome compliance measures.

(E) Share experiences and innovative approaches related to information sharing and information security best practices that span both defensive operational security such as penetration testing regimes, and incident response mitigation, and span security policies compliance, such as FISMA.

(F) Identify common Computer Information Security Officer (CISO) and information assurance professional qualifications in coordination with the FCIOC IT Workforce Committee.

3. Leadership:

The OMB Office of Electronic Government Administrator shall select co-chairpersons for the ISIMC from the FCIOC.

The co-chairpersons for the ISIMC shall select an Executive Secretary.

4. Membership:

Membership shall be comprised of the following members:

- (A) Two co-chairpersons selected by the OMB Office of Electronic Government Administrator;
- (B) A Government employee representative from the Department of Homeland Security, Cybersecurity & Communications;
- (C) A Government employee representative from the Office of the Director of National Intelligence (ODNI);
- (D) A Government employee representative from the Committee on National Security Systems (CNSS);
- (E) A Government employee representative from the National Institute of Standards and Technology (NIST);
- (F) The CIO and/or CISO of each cabinet-level agency (25 agencies) that are represented on the FCIOC and derived from the Federal Information Security Management Act (FISMA) and the Clinger Cohen Act (CCA) (otherwise known as the Information Management and Technology Reform Act (IMTRA));
- (G) The CIO and/or CISO of the Department of the Army, the Department of the Navy, and the Department of the Air Force, if chief information officers have been designated for such departments;
- (H) A Government employee representative from the United States Strategic Command;
- (I) A Government employee representative from the United States Computer Emergency Readiness Team;
- (J) A Government employee representative from the Intelligence Community Incident Response Center;
- (K) A Government employee representative from the Small Agency CIO Council;

Information Security and Identity Management Committee (ISIMC) Charter

- (L) The team lead/chair of ISIMC approved subcommittees and/or working groups; and
- (M) Any other officer or employee of the United States designated by the ISIMC co-chairpersons, such as representatives from other Federal committees.

5. Subcommittees, Working Groups and Task Forces.

The co-chairs of the ISIMC establish subcommittees, working groups, and task forces as necessary.¹ The four standing subcommittees, established by the ISIMC co-chairs, are as follows:

- (1) Security Program Management Subcommittee (SPMSC);
- (2) Identity, Credential and Access Management Subcommittee (ICAMSC);
- (3) Network and Infrastructure Security Subcommittee (NISC); and
- (4) Security Acquisitions Subcommittee (SASC);

6. Responsibilities:

(A) Co-Chair(s):

The co-chairs provide strategic direction and tactical leadership to the review, coordination, and integration of initiatives. The co-chairs are responsible for the following activities:

- (1) Determine and lead the decision making process to be followed by the Committee;
- (2) Approve actions, recommendations, and ISIMC work products;
- (3) Approve meeting agendas;
- (4) Lead ISIMC meetings;
- (5) Encourage consensus among Committee members and work to resolve any differences;
- (6) Consider ISIMC member votes, in the absence of consensus, when approving or recommending an action or position; and
- (7) Arrange for minutes to be taken at each meeting, distribution of meeting materials, and other meeting-related tasks;

(B) Committee Members:

Committee members are responsible for the following activities:

- (1) Attend each ISIMC monthly meeting. If the member cannot be present at a meeting, the member may send an email to the co-chair designating an alternate who can represent the agency and assume the member responsibilities in the absence of the member;
- (2) Reach consensus among members and work to resolve any differences;
- (3) Vote for concurring or non-concurring on issues, actions, and deliverables if consensus can not be reached;
- (4) Ensure participation in policy activities, initiatives, and solutions ;
- (5) Identify and recommend ISIMC sub committees and working groups as needed; identify agency resources that can assist and lead ISIMC working groups; and assist in developing their charters and reviewing their work products; and
- (6) Communicate and coordinate best practices to ensure policy and implementation alignment.

¹ Subcommittees are established as long standing groups that do not have an end date and whose functions rarely change. Working groups are established to address tactical and strategic SIMC initiatives of limited duration. Task forces are established to address an immediate tactical need and are of short duration.

Information Security and Identity Management Committee (ISIMC) Charter

(C) Executive Secretary:


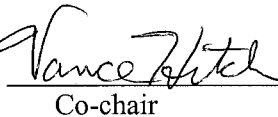

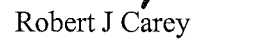
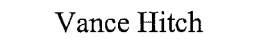
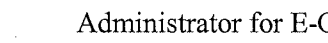
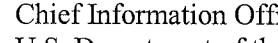
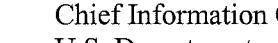
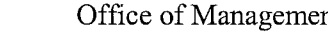
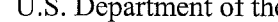

The Executive Secretary is responsible for the following activities and other such responsibilities as designated by the ISIMC co-chairs:

- (1) Introduces issues that need to be resolved either within the ISIMC, by individual partner agencies, ISIMC subcommittees, working groups and task forces;
- (2) Prepares a meeting agenda and solicits input from ISIMC members, subcommittees, working groups and task forces. The agenda will be coordinated with the co-chairs prior to its distribution. The agenda will be distributed to each ISIMC member at least one business day before each meeting;
- (3) Ensures that meeting minutes are maintained and distributed to the ISIMC members.
- (4) Coordinates/develops products at the direction of the ISIMC.

EFFECTIVE DATE

This charter is effective as of the date signed and remains in effect until modified or rescinded.

SIGNATURES

 Co-chair	 Co-chair	 Karen Evans
 Robert J Carey	 Vance Hitch	 Administrator for E-Government
 Chief Information Officer	 Chief Information Officer	 Office of Management and Budget
 U.S. Department of the Navy	 U.S. Department of Justice	