# DHS Information Sharing and Safeguarding Strategy

*January 2013*

Homeland Security

# Table of Contents

# Preface

The Department of Homeland Security (DHS) *DHS Information Sharing and Safeguarding Strategy (Strategy)* sets forth the Department's information sharing and safeguarding direction and priorities for the Homeland Security Enterprise (HSE) in the coming years. This *Strategy* supports the policy positions set forth by the White House in the *National Strategy for Information Sharing* (2007), as well as the *National Strategy for Information Sharing and Safeguarding* (2012), and presents how the Department will enable its missions through sharing and safeguarding information. A specific section in the *Strategy* outlines our alignment to the *National Strategy for Information Sharing and Safeguarding.*

The vision and mission sections of the *Strategy* present a compelling picture that DHS can strive for in the future and provide the purpose of sharing and safeguarding across the HSE in the coming years, respectively. The next sections provide our five capstones—necessary underpinnings to achieve the vision and mission—as well as four long-term outcomes in the form of goals that help DHS achieve its mission. Each goal has related objectives and objective elements that identify specific, broad-based outcomes that DHS is to achieve. These outcomes also provide the necessary guidance for the prescribed implementation plan that shall be developed within 90 days of issuance.

The *Strategy* demonstrates that DHS has reached a level of maturity where performance measures *must* be developed to demonstrate the results that sharing and safeguarding efforts have achieved. Our success in gauging our performance will both allow us to make decisions that are more informed during implementation and be the ultimate indicator of effective and efficient mission enablement.

# Message from the Secretary

While we have made important progress in securing our Nation since the tragic attacks on September 11, 2001, we continue to face persistent and evolving threats. We have learned as a Nation that we must maintain a constant, capable, and vigilant posture to protect ourselves against new threats and evolving hazards. Ensuring all of those who protect the Homeland have and share the necessary information to execute our missions is the seminal reason why DHS was established.

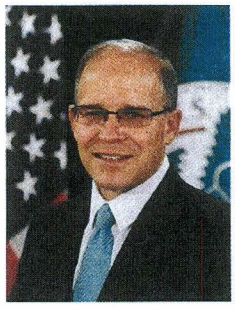
Over the past two years, the Department has been working diligently with our homeland security partners to build a new architecture to execute our missions. The four essential elements of the distributed homeland security architecture—The National Network of Fusion Centers, the Nationwide Suspicious Activity Reporting Initiative, the National Terrorism Advisory System, and the *"If You See Something, Say Something™"* campaign—learn from and build on each other. These four elements require the engagement of the extended Homeland Security Enterprise to be successful.

The purpose of the *DHS Information Sharing and Safeguarding Strategy* is to outline goals and objectives that guide the activities of participants in the Homeland Security Enterprise towards a common information sharing and safeguarding end within the context of our distributed homeland security architecture. With this *Strategy*, I ask the Department's Information Sharing and Safeguarding Governance Board to begin the next chapter in maturing the Department toward establishing clear, manageable guidelines for our mission operators that better enable all of us to manage the associated risks with sharing and safeguarding information.

Yours very truly,

Janet Napolitano

# Message from the Chair of the Information Sharing and Safeguarding Governance Board



In the past decade, the United States has made significant progress in safeguarding our Homeland. Much of this is due to embracing not only a whole of government, but also a whole of society approach to homeland security. The threats facing our country have evolved significantly since September 11, 2001 and continue to do so. We must remain nimble and steadfast in our approach.

With the commemoration of the 10th anniversary of September 11, 2001 attacks behind us, it is a good time to present the *DHS Information Sharing and Safeguarding Strategy* for serving the Homeland Security Enterprise. Since the Information Sharing Governance Board issued our last plan in 2008, the Department made great progress in establishing the foundational elements needed to define and oversee the DHS Information Sharing Environment. Our sharing and safeguarding environment has also changed over the past three years. As a result, focusing on the needs of mission operators is more important now than ever before and there are new national policies and practices surrounding the handling of information to manage and reduce risk.

This *Strategy* marks the beginning for DHS to lead the Homeland Security Enterprise, redoubling our efforts across all the Components and Offices to focus on action and delivering tangible outcomes that better enable our personnel to respond effectively to rapidly evolving threats. It establishes the vision, mission, goals, and objectives for sharing and safeguarding information as well as managing the associated risks. The *Strategy* not only paves the way for a more detailed effort to achieve the goals and realize the vision, but uses indicators and measures to report mission outcomes and impact as well. The end state of this Strategy is the establishment of the DHS Information Sharing Environment which will enable a comprehensive and streamlined ability to share and safeguard critical information across the Homeland Security Enterprise.

Time is of the essence. Improvements must be made rapidly to build on our recent progress and improve our ability to support and guide those who protect the Homeland.

Sincerely,

William E. Tarry, Jr.

# Background

The 2005 *Information Sharing at the Department of Homeland Security* memorandum initiated the Department's approach to meeting the information sharing needs of the Homeland Security Enterprise (HSE).[1] The recommendations in this memorandum served as the foundation for DHS information sharing governance. The *DHS Policy for Internal Information Exchange and Sharing* memorandum, issued in February 2007, identified, in part, the Information Sharing Governance Board (ISGB) and directed it—in coordination with the General Counsel, the Privacy Officer, and the Officer for Civil Rights and Civil Liberties—to work closely with other DHS Components to monitor DHS information management processes ensuring that privacy, civil rights and civil liberties, and other legal protections are fully respected. In April 2007, the Department established the ISGB as the executive decision-making body within a tiered governance structure dedicated to improve DHS's sharing of information with both internal and external stakeholders. DHS published its first information sharing strategy in 2008 (*2008 Strategy*).[2]

**KEY TERMS**

- ***Vision*** is a compelling picture that DHS can strive for in the future.
- ***Mission*** is the purpose of the sharing and safeguarding across the HSE.
- ***Capstones*** are necessary principles to achieve the vision, mission, and goals.
- ***Goals*** are long-term outcomes that help DHS achieve its mission.
- ***Objectives*** are broad based outcomes that indicate DHS's achievement of the goals.
- ***Key Objective Elements*** are methods DHS can use to achieve key outcomes. These will form the basis for the implementation plan.
- ***Indicators*** are broad-based metrics that show whether results are trending in the desired direction.
- ***Measures*** help determine the impact of activities and should inform leadership decisions.

The *Quadrennial Homeland Security Review (QHSR)* identified the missions and focus of the HSE as:[3]

1. Preventing Terrorism and Enhancing Security;
2. Securing and Managing Our Borders;
3. Enforcing and Administering Our Immigration Laws;
4. Safeguarding and Securing Cyberspace;
5. Ensuring Resilience to Disasters; and
6. Maturing and Strengthening the Homeland Security Enterprise.

---

[1] The Under Secretary for Policy and International Relations, the Assistant Secretary of Intelligence and Analysis (I&A) (now known as the Under Secretary for I&A), the Director of Operations, and the Chief Information Officer delivered the Information Sharing at the Department of Homeland Security memorandum to the Secretary on 16 December 2005.

[2] DHS, *Information Sharing Strategy*, April 2008.

[3] The QHSR defines "homeland security enterprise" as the "collective efforts and shared responsibilities of federal, state, local, tribal, territorial, nongovernmental, and private-sector partners—as well as individuals, families, and communities—to maintain critical homeland security capabilities." [*QHSR*, February 2010, p. 12]. In addition to the missions, the QHSR calls for the "maturing and strengthening the homeland security enterprise." The Department recently issued the *U.S. Department of Homeland Security Strategic Plan for FY 2012-2016*, building on the conclusions of the QHSR and the Bottom-Up Review to include goals, objectives, and key performance indicators.

The unlawful disclosure of classified information by WikiLeaks in the summer of 2010 has rightfully renewed the Department's focus on risk management across the HSE. On 7 October 2011, the President issued Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, which, in part, requires all federal departments and agencies to institute a governance mechanism to synchronize information sharing and safeguarding. Accordingly, the ISGB revised and approved its updated charter in October 2011 with some of the following changes:

- Renamed the ISGB to the Information Sharing and Safeguarding Governance Board (ISSGB, Board);
- Expanded the scope of the Board to serve as the DHS governance mechanism for both information sharing and safeguarding;
- Expanded Board membership to incorporate Components and Offices with information safeguarding responsibilities; and
- Reaffirmed the role of the Under Secretary for Intelligence and Analysis as the ISSGB Chair and recognized the role of the DHS Chief Information Officer (CIO) as Vice Chair.

The ISSGB, Information Sharing Coordinating Council (ISCC), and Information Safeguarding and Risk Management Council (ISRMC) as well as the Executive Steering Committees (ESCs), Shared Mission Communities (SMCs), Integrated Project Teams (IPTs) comprise the tiered information sharing and safeguarding governance structure.[4] The ISSGB directs and provides oversight to the ISCC and ISRMC to develop and implement policies and procedures for information sharing (e.g., ISCC) and develop and implement policies and procedures for information safeguarding (e.g., ISRMC).[5]

This publication replaces the *2008 Strategy*. All ISSGB members were invited to participate in developing this *Strategy* and used the strategic planning framework depicted in the figure below.[6] This approach is grounded in government and commercial best practices. Through this lens, the ISSGB can best understand and connect the needs of mission operators with individual implementation tasks. The ISSGB can further ensure that (1) these efforts are both aligned to enable the *Strategy's* objectives, goals, and vision and (2) indicators and measures are in place to demonstrate and report progress and results to key HSE stakeholders.

[4] ESCs provide oversight and guidance to identified information sharing programs. SMCs are mission-focused forums to identify and address common challenges. IPTs are responsible for implementation of specific projects in support of ISCC and ISRMC initiatives. In practice, the ESCs, SMCs, and IPTs generally coordinate through the ISCC and ISRMC when engaging the ISSGB.

[5] *Ibid.*

[6] Framework is based on requirements found in the *Government Performance and Results Act of 1993 (GPRA*) and *Government Performance and Results Modernization Act of 2010 (GPRAMA)* (align goals and objectives in a "line of sight" to demonstrate how performance contributes to organizational objectives and goals in service of the mission), as well as other commercial and government management best practices.

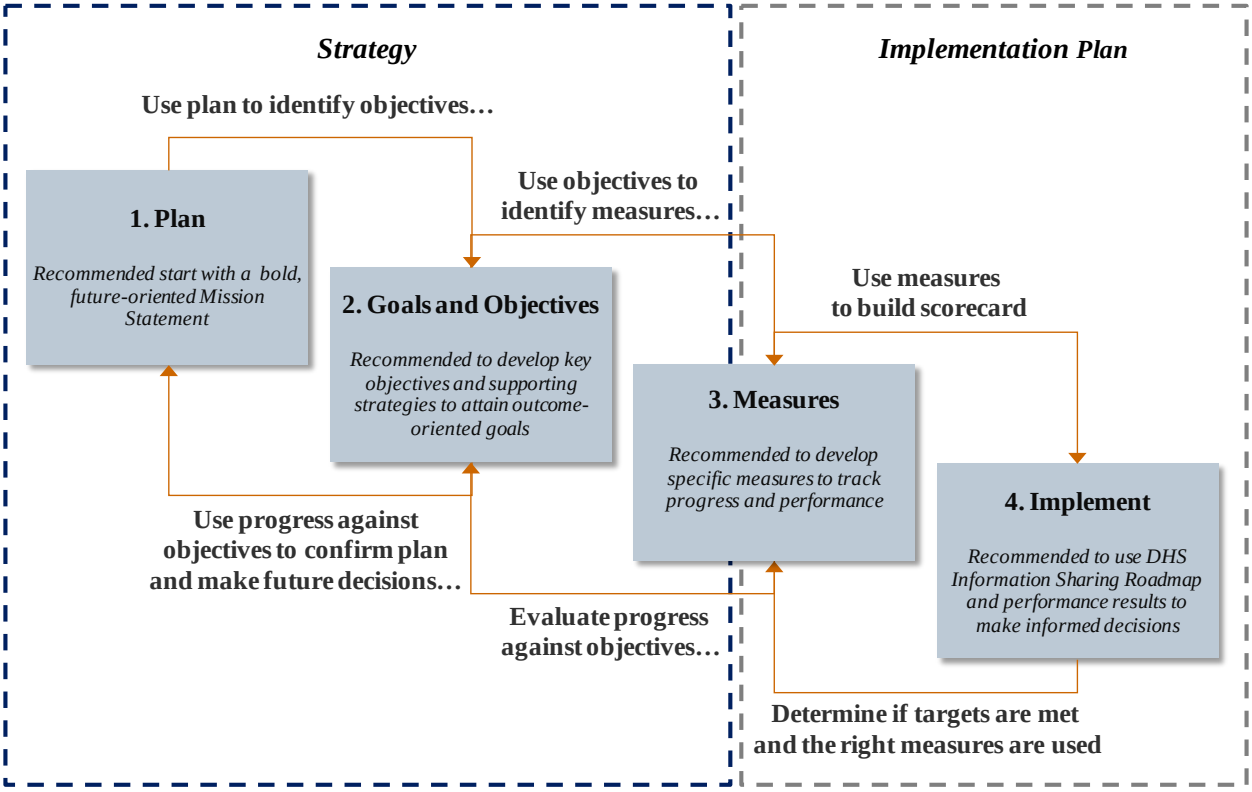



**Figure 1: Strategic Planning Framework**

This *Strategy* addresses steps 1 and 2 of the framework (*see, infra,* Sections III through VI) and provides guidance for steps 3 and 4 (*see, infra,* Sections VII and VIII).

# I. Vision

***DHS shall serve as a leader across the HSE in sharing and safeguarding information and managing the associated risk through the establishment of the DHS Information Sharing Environment (DHS ISE).***

> To prevent acts of terrorism on American soil, we must enlist all of our intelligence, law enforcement, and homeland security capabilities. […] We are improving information sharing and cooperation by linking networks to facilitate federal, state, and local capabilities to exchange messages and information seamlessly, conduct searches, and collaborate.
>
> *President Obama's National Security Strategy, May 2010*

DHS's information sharing and safeguarding vision provides a compelling and comprehensive picture of the organization's future—its end state. For FY 2013–2018, DHS's information sharing and safeguarding efforts will build upon the ISSGB's vision of April 2010 to encompass the Department's missions, pointing towards a future where systems support decisions that securely provide the "right information" to the "right people" at the "right time" in a manner that rigorously protects personally identifiable information, privacy interests, civil

rights, and civil liberties.[7] The DHS ISE is defined as an interface that lets users appropriately find the people and data necessary to perform their job and lets them know (1) what information is available; (2) what authorizations are required; and (3) the terms under which they may use shared information.[8]

# II. Mission

***Facilitate homeland security mission success through the timely and informed sharing and safeguarding of information.***

DHS Components, Offices, and personnel must further share and safeguard information essential to the operational success of those tasked with the safety and security of our nation while maintaining appropriate privacy, civil rights, and civil liberties protections. Through our missions, we will follow the White House's direction in the *National Security Strategy* to further "integrate homeland security with national security."[9]

# III. Capstones

The following capstones (e.g., principles) are the necessary underpinnings for DHS to achieve its information sharing and safeguarding vision, mission, and goals.

1. ***Capstone #1:*** *Manage information as a national asset.*
   - Information sharing and safeguarding are force multipliers that enable the HSE to achieve its mission objectives faster and at reduced risk and cost.
   - Establish simple and consistent rules (e.g., authorities and constraints) to assist sharing and safeguarding information in DHS missions.
   - Make information available to those who need it, while simultaneously keeping it secure from unintended or intended misuse.

2. ***Capstone #2:*** *Embrace a risk-informed culture that responsibly shares and safeguards information.*
   - Create a culture of "information stewards" to eliminate the divide between information "users" and information "owners" through a trusted risk management environment.
   - Instill confidence in the security and integrity of information through fostering trust and collaboration across the HSE, as sharing and safeguarding information are complementary processes.

[7] On 29 April 2010, the ISGB approved the following vision: "By September 30, 2015, DHS will transform the Department's people, policies, and processes/technologies to enable the consistent successful execution of the five core homeland security missions and further mature and strengthen the homeland security enterprise's information sharing environment to ensure that the right information gets to the right people at the right time in a manner that rigorously protects privacy and civil liberties." With the accomplishments achieved since April 2010 and the addition of the Safeguarding mission in the Fall 2011, the Department's vision was updated accordingly.
[8] *DHS Information Sharing Segment Architecture (ISSA)*, Vol. 1, Pg. 2, 15 May 2009.
[9] *National Security Strategy*, White House, May 2010, p. 2.

- Maintain the integrity and security of shared information.

3. ***Capstone #3:*** *Protect individuals' personally identifiable information, privacy, civil rights, and civil liberties.*
   - Support and enhance mechanisms to ensure individuals' personally identifiable information, privacy rights, civil rights, and civil liberties protections as well as sustain the trust of HSE personnel and the U.S. public.

4. ***Capstone #4:*** *Promote information sharing among our homeland security partners across the HSE through training, implementation of incentives, providing the requisite tools to share and safeguard, and fostering collaboration.*
   - Expand appropriate information sharing with our federal, state, local, tribal, territorial, international, public, and private sector partners through strengthening, enhancing, and extending the distributed homeland security architecture, inclusive of the following elements:
     - National Network of Fusion Centers;
     - Nationwide Suspicious Activity Reporting Initiative (NSI); and
     - National Terrorism Advisory System.

5. ***Capstone #5:*** *Implement this Strategy as a top Departmental priority that enables leadership across the HSE to make decisions that are more informed.*
   - The purpose of sharing information is to inform decision-making and resource allocation decisions, linking information with operations to support situational awareness, joint planning, and mission execution.
   - Informed decision-making is dependent upon the discovery, retrieval, and use of accurate, trusted, relevant, actionable, and timely information.
   - Ensure safeguarding considerations are addressed and integrated in support of informed sharing decisions to maintain the integrity of shared information and confidence that information can be shared without fear of compromise, modification, or manipulation, regardless of the intended recipients.
   - Leadership endorses this *Strategy* and it is to be practiced by all. Executing the *Strategy* is an ongoing endeavor that will better enable our homeland security partners across the HSE to protect the Homeland.
   - Active participation in and adherence to Information Sharing and Safeguarding Governance, creating a singular platform for the consideration and communication of DHS ISE priorities and initiatives.

# IV. Goals and Objectives

***<u>Goal 1 - Share</u>: Provide all those who protect the Homeland with the policies, standards, and guidelines to institutionalize the efficient, effective, and appropriate sharing of information needed to accomplish DHS missions.***

***Objective 1.1 - Better Equip Mission Operators to Share Appropriately:*** *Ensure Department personnel and HSE partners have the knowledge, skills, and capabilities needed to share information timely, appropriately, and in an effective and efficient manner.*

***Key Objective Elements***

*1.1.1. Improve governance to identify and remove barriers to collaboration and foster better decision making, performance, accountability, and implementation while consolidating and streamlining access to information across the Department*

- The ISSGB, through the ISCC and ISRMC shall drive decisions and priorities for information sharing and safeguarding in a manner that is clear, understood, and reconciled.
- Create, publish, and fully implement the Information Sharing Segment Architecture (ISSA) to enhance the Department's ability to gather, access, and safeguard information and mature the use of common processes and standards to ensure that DHS will participate in the Federal ISE.
- Ensure HSE stakeholders external to DHS receive information in a timely manner to enable mission accomplishment.

> The threats against the American people and our institutions have compelled us to accelerate responsible information sharing across every level of government. The operators, analysts, and investigators who protect our nation need access to the right information at the right time, shared in a secure manner.
>
> *Kshemendra Paul, Program Manager, Information Sharing Environment, 30 June 2011*

*1.1.2. Establish and/or document cross-HSE information sharing activities to identify shared mission objectives and best practices*

- Identify and/or refine, document, and publish information sharing activities that cross organizational boundaries (e.g., information flows) to better help operators understand their shared objectives and more efficiently and effectively enable the HSE missions, to include an alignment of privacy rights, civil rights, and civil liberties protections.
- Complete the implementation of the NSI programs in the National Network of Fusion Centers and federal entities while expanding training and outreach beyond law enforcement to the rest of the public safety community.
- Achieve the four Critical Operational Capabilities, four Enabling Capabilities, and other prioritized objectives, across the National Network of Fusion Centers to enable effective and lawful execution of their role as a focal point within the

state and local environment for the receipt, analysis, gathering, and sharing of threat-related information.

***Objective 1.2 -Issue Policy, Guidance, and Standards:*** *Ensure Department personnel and HSE partners have the appropriate policy, guidance, and standards necessary to facilitate effective and efficient information sharing.*

***Key Objective Elements***

*1.2.1. Clarify and streamline mission execution in a consistent manner through policies as well as common processes, procedures, and standards*

- Provide policies (e.g., Directives, memoranda, etc.) that clarify and streamline the implementation and execution of the information sharing and safeguarding mission, including defined roles and responsibilities.[10]
- Examine, coordinate, and update (as necessary) DHS policies, processes, and procedures within DHS and in relationships between DHS and other federal agencies; state, tribal, local, and territorial governments; and private sector and international partners to establish sector specific protocols, so that DHS expresses "one view" on information sharing and collaboration issues and improve information quality and timeliness.[11]
- Define and implement common processes and standards using machine-readable policies to support automated authorized discovery and access decisions.
- Adopt government-wide common processes for Requests for Information, Alerts, Warnings, and Notifications to enable timely receipt and dissemination of information and appropriate response.
- Develop and promote common metadata tagging standards to facilitate federated search, discovery, access, correlation, and data monitoring across the Federal government, its networks, and security domains.
- Develop a distributed and decentralized data aggregation reference architecture for a consistent approach to data discovery and correlation across disparate datasets.
- Define and deploy baseline capabilities and common requirements to enable data, service, and network interoperability.
- Enhance HSE-wide data correlation to enable users to reference authoritative, up-to-date information across holdings to identify relationships among people, places, things, and characteristics that are otherwise not obvious.
- Reuse common, existing standards in our information sharing and safeguarding efforts to benefit from the prior time, resources, and experience invested to fully vet and implement a standard.

[10] *See ISSGB Charter*, Responsibility "C," November 2011.
[11] *See ISSGB Charter*, Responsibility "D," November 2011.

*1.2.2. Facilitate effective and efficient information sharing through agreements, training, technical assistance, and incentives*

- Provide guidance for Components and Offices to actively streamline, manage, and arbitrate the development and execution of Information Sharing and Access Agreements (ISAAs), to include the Memoranda of Agreements, Memoranda of Understanding, Letters of Intent, and other data agreements between and among the Department and its Components; other federal agencies; and state, tribal, local, territorial, private sector, and international partners.[12] DHS shall apply the common procedures it adopted in April 2010 to implement a streamlined process that effectively and efficiently strengthens DHS-wide sharing and safeguarding while protecting personally identifiable information, privacy, civil rights, and civil liberties.[13]
- Increase awareness and implementation of information sharing values through training, technical assistance, monitoring, and performance evaluation of staff and applicable HSE partners to enable the full potential of their contributions.
- Ensure all applicable employees promote responsible information sharing and compliance with applicable law and policies through demonstration of information sharing behaviors contained in Competencies currently listed in their Performance Work Plan.[14]
- Create an annual *ISSGB Information Sharing and Safeguarding Award* to be awarded to the cross-HSE initiative that provided the greatest value to the HSE.

*1.2.3. Support the Department's intra- and inter-agency engagement*

- Support the ISA IPC, the National Security Staff, and the PM-ISE on behalf of ISSGB members.[15]
- Formalize relationships with other intra- and inter-agency councils.[16]

***Goal 2 - Safeguard: Protect information and information systems and networks against unauthorized access, modification, disclosure, and use.***

Safeguarding relates to the measures used to deter, detect, and prevent against the loss, misuse, theft, unauthorized access, unauthorized modification, unauthorized disclosure, or unauthorized use of classified, controlled unclassified information (CUI), and other unclassified information of a sensitive nature, and the protections afforded to information systems/networks

[12] *See ISSGB Charter*, Responsibility "J," November 2011.
[13] On 29 April 2010, the ISGB approved the "DHS Data Sharing Framework." The Board instructed Components and Offices to use this uniform approach to: (1) working towards completing ISAAs (concept to execution) in weeks rather than months; (2) monitor and enforce agreements' terms and conditions through a standardized, centrally managed approach; and (3) automatically alert parties when changes occur to laws, policies, and/or operating environment that may impact agreements.
[14] DHS Deputy Secretary Memorandum, *Inclusion of Information Sharing Competencies in Employee Performance Appraisals*, 10 July 2009.
[15] *See ISSGB Charter*, Responsibility "E," November 2011.
[16] *Ibid.*

on which such information resides.[17] Safeguarding encompasses—but is not limited to—counterintelligence, information assurance, information security, operational, administrative, personnel, and physical security, as well as privacy, civil rights, and civil liberties protections.

***Objective 2.1 - Provide Information Security:*** *Protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide for confidentiality, integrity, and availability.*[18]

***Key Objective Elements***

*2.1.1. Establish and implement removable media policies to enhance security and mitigate associated risk*

- Ensure DHS establishes and implements policies that incorporate the United States Computer Emergency Readiness Team and other recommended best practices (e.g., lock down, data loss prevention, and alerts), regarding removable media devices to enhance security and mitigate associated risk.[19]

> Our nation's security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely.
>
> *Executive Order, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," 7 October 2011*

*2.1.2. Reduce user anonymity through improved identity, authentication, and authorization controls as well as Web site consolidation*

- Ensure DHS positively identifies system or network users and all user access to information resources (e.g., authentication) and reduces the number of DHS Web sites with classified information by consolidation.
- Implement Public Key Infrastructure for access control (e.g., consolidate DHS classified Web sites).

*2.1.3. Develop clear policies, procedures, and common standards that extend Federal Identity, Credential, and Access Management (FICAM) across all security domains allowing discovery and access of useful information*

- Permit users to discover and access information that may be useful to their mission, within the scope of their duties, responsibilities, clearance, and responsibility to share while preventing unauthorized access to information.

---

[17] CUI refers to information categorized as such pursuant to directives issued in accordance with Executive Order 13556, *Controlled Unclassified Information.* As of the publication date of this strategy, CUI and its safeguarding framework have not yet been implemented.

[18] *See ISRMC Charter,* October 2011; *see also* Committee on National Security Systems, *CNSS Instruction No. 4009 - National Information Assurance Glossary*, 26 April 2010.

[19] "Lock down" refers to controls that restrict or lock down access to devices that could permit the removal of data from a computer, such as a floppy or CD/DVD drive, or a USB port; "Data Loss Prevention" refers to software which monitors and detects data being written to external media or transferred out of an organization (e.g., e-mail), and "alerts" refer to real time, automated alerts that a user is attempting to subvert lock down or data loss prevention policies.

- Enhance safeguarding efforts across the HSE through data-level controls, automated monitoring, and cross-domain solutions.
- Extend and implement the FICAM Roadmap across all security domains.

*2.1.4. Document, monitor, and analyze system actions through enterprise audit capabilities*

- Increase system logging to reflect all successful and unsuccessful attempts to log in, to access, insert, modify, delete, copy, transfer, or print information and other meaningful user and system actions, and transfer the audit logs to a centralized storage device and audit server for further monitoring and analysis.

***Objective 2.2 - Provide Administrative, Operational, Physical, and Personnel Security:*** *Protect DHS information and information systems/networks through complementing and integrating the technical measures that assure information security with the administrative, operational, physical, and personnel security measures necessary for a harmonized and holistic safeguarding framework.*[20]

***Key Objective Elements***

*2.2.1. Deter, detect, and mitigate insider threats through the development of structural reforms as well as policies and procedures*

- Activities to include the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure.[21]
- Establish policies and procedures to integrate security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices.

*2.2.2. Control physical access to systems, networks, facilities, and information resources*

- Ensure physical user access to systems, networks, facilities, and information resources are controlled via physical, hard token authentication mechanisms (e.g., facility physical security measures against SIGINT efforts).

*2.2.3. Ensure administrative and physical security where classified information is processed*

- Ensure HSE-wide compliance with appropriate standards for the handling and storage of classified information and information systems/networks on which classified information is processed.

*2.2.4. Ensure security screening for personnel*

- Ensure persons who require access to classified or sensitive unclassified information are subject to the appropriate level of security investigation and continuous evaluation.

[20] *See ISRMC Charter*, October 2011; *DHS Instruction Manual 121-01-010: Physical Security*, 24 November 2009; *121-01-011: Administrative Security Program; and 121-01-007, Personnel Suitability and Security Program.*
[21] *See* Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, Section 6, 7 October 2011.

*2.2.5. Train personnel to appropriately safeguard information and resources*

- Ensure all persons with access to classified or sensitive unclassified information and with access, rights, and privileges to information systems/networks are afforded the training necessary to safeguard information and resources appropriately and to accomplish their missions with confidence and in compliance with safeguarding standards.

***Objective 2.3 - Protect Personally Identifiable Information, Privacy, Civil Rights, and Civil Liberties Protections:*** *Guide and direct DHS users of DHS data to protect information in a manner that protects privacy interests, civil rights, and civil liberties.*[22]

***Key Objective Elements***

*2.3.1. Develop and issue safeguarding guidance that protects privacy interests, civil rights, and civil liberties*

- Develop and issue guidance that informs DHS personnel how and why to safeguard DHS information, with whom, and under what circumstances it should be shared.

*2.3.2. Build privacy protections into the development of information sharing operations*

- Ensure privacy, civil rights, and civil liberties are addressed early in the planning of any new initiative (or in the redesign of existing systems and processes) to allow information protections to be considered, managed, and monitored in a more efficient and effective manner across the DHS ISE.
- Ensure privacy, civil rights, and civil liberties are addressed in data element level tagging (*see, infra*, Key Objective Element 1.2.1.).

*2.3.3. Develop and implement controls*

- Implement controls in a manner that safeguards information and protects privacy interests, civil rights, and civil liberties.

*2.3.4. Train personnel*

- Provide information sharing safeguarding, and handling training to appropriate stakeholders using a common curriculum tailored to promote consistent, yet flexible, and trusted processes and protect privacy interests, civil rights, and civil liberties.

*2.3.5. Conduct compliance reviews to ensure privacy compliance, increase consistent application of privacy protections, and promote accountability across the DHS ISE, and integrate with self-inspection and security compliance review programs*

- Ensure all information sharing access agreements include appropriate privacy, civil rights, and civil liberties protections.
- Ensure all information sharing access agreements are appropriately coordinated with oversight offices to ensure appropriate safeguarding provisions are built into the agreements.

[22] *See ISRMC Charter*, October 2011.

- Ensure all information sharing access agreements incorporate safeguarding provisions whereby parties conduct or undergo audit or compliance reviews to ensure DHS data is protected appropriately and information is used in a manner that respects privacy interests, civil rights, and civil liberties.
- Ensure all information sharing and safeguarding programs/initiatives complete any required privacy, civil rights and civil liberties compliance reviews.

*2.3.6. Promote accountability for the consistent applications of protections across the DHS ISE*

- Ensure that enterprise audit capabilities address privacy, civil rights, and civil liberties sensitive data.

***Objective 2.4 - Governance and Oversight:*** *Institutionalize oversight to guide users, foster accountability, and oversee/monitor user activity with limited impact on mission and commerce.*[23]

***Key Objective Elements***

*2.4.1. Provide sustained focus on safeguarding information through the ISRMC and/or other applicable governance bodies*

- The ISRMC shall work through the ISSGB, DHS Office of the Chief Information Officer (OCIO), DHS Office of the Chief Security Officer, and/or authorizing officials as appropriate to provide sustained focus on safeguarding information consistent with its Charter and public law, all current and future Presidential Decision Directives, Homeland Security Directives, Intelligence Community (IC) and Committee on National Security Systems (CNSS) Directives, Policies, Instructions, and other authoritative guidance.[24]

*2.4.2. Represent DHS information safeguarding equities across the HSE and inter-agency*

- Maintain liaison and cooperation with other security management committees/boards, including, but not limited to the DHS, IC, CNSS, Federal CIO Council, etc.

*2.4.3. Oversee the Department's dispute resolution process and procedures*[25]

- Ensure existing processes conform to mandates, are known across the HSE, and are available, efficient, timely, and easy to use.
- Foster an environment that recognizes and supports the ISSGB's ability to speak on behalf of the DHS ISE.

*2.4.4. Develop and implement self-inspection and security compliance review programs*

[23] *See ISRMC Charter,* October 2011.
[24] *Ibid* (The ISRMC has a Department-wide scope for National Security Systems as defined in 44 U.S.C. § 3542(b)(2), and includes any system or network that stores, processes or transmits classified national security information as defined in Executive Order 13526, to include standalone systems).
[25] *See ISSGB Charter,* Responsibility "F," November 2011. The ISCC created the "DHS Information Sharing Dispute Resolution Process" in 2009 to establish the processes and procedures for resolving information sharing conflicts within DHS. The ISGB approved this Process during its 8 May 2009 meeting.

- Ensure implementation of a self-inspection program as required by Executive Order 13526 and DHS Instruction 121-01-011.
- Ensure execution of multi-discipline compliance reviews of DHS Component administrative security, personnel security, physical security, industrial security, operations security, special security, and counterintelligence programs.

*2.4.5. Ensure Departmental actions limit impact on mission and commerce*

- Coordinate with partners to ensure safeguarding efforts maintain information integrity and do not detract from accomplishing the Department's missions and support national and economic security without impeding the flow of commerce.

***Goal 3 - Manage and Govern Risk: Provide the policies, metastandards, processes, and tools to efficiently and effectively identify and manage the risks associated with sharing and safeguarding classified, controlled unclassified, and other information which DHS has a responsibility to safeguard.[26]***

***Objective 3.1- Establish and Implement a Risk Management Strategy and Framework:*** *Establish an information sharing and safeguarding risk management strategy and framework that supports an appropriate risk-management posture (acceptance of the risk and identification of DHS's risk tolerance) to build trust requiring the ability to manage rather than avoid risk..*[27]

As the *Quadrennial Homeland Security Review* identified, homeland security is about effectively managing risks to the nation's security, including from acts of terrorism, natural and manmade disasters, cyber attacks, and transnational crime. DHS plays a leadership role in the nation's unified effort to manage risks working across the homeland security enterprise, which includes federal, state, local, tribal, territorial, nongovernmental, and private sector partners.

*Secretary Napolitano, DHS Policy for Integrated Risk Management, 27 May 2010*

***Key Objective Elements***

*3.1.1. Define the principles and processes of homeland security risk management and what they mean in the context of sharing and safeguarding information*

*3.1.2. Promote a common understanding of and approach to sharing and safeguarding risk management to include the policies, guidance, standards, processes, and priorities necessary to manage effectively and efficiently the risk associated with sharing and safeguarding classified, controlled unclassified, and other legally protected information and information systems*

*3.1.3. Establish a common foundation that enables consistent risk management application and training for mission operators to mitigate the risks of sharing and not sharing*

[26] *See ISRMC Charter,* October 2011 (scope limited to classified information).
[27] DHS, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine,* April 2011.

*3.1.4. As part of the larger DHS effort on risk management, support the development of a risk management culture to establish a greater level of trust among HSE organizations*

***Objective 3.2 - Institutionalize Risk Management and Monitor Mission Impact:*** *Institutionalize and continuously monitor how the information sharing and safeguarding risk management strategy affects DHS missions.*

***Key Objective Elements***

*3.2.1. Institutionalize risk management into daily mission operations as a priority and an integral part of how DHS conducts its business*

- Establish the context for risk-based decisions.
- Assess risk (e.g., threat, vulnerabilities, likelihood, and consequences/impact).
- Identify how DHS will address risk, including the implementation of policies and standards, increased awareness and comprehensive training, governance, and accountability.
- Monitor and report on risk over time with evolving mission needs/environments.

*3.2.2. Establish and operate a risk-management governance structure that addresses sharing and safeguarding of controlled unclassified and other legally protected information*

- Align strategic risk management decisions with missions and business functions consistent with DHS goals and objectives.
- Define and execute risk-management processes and capabilities to frame, identify, respond to, monitor, and report on DHS operations and assets, individuals, other organizations, and the nation.
- Establish risk management roles and responsibilities.

> Effective and efficient information sharing and access are essential to enhancing the national security of the United States and the safety of the American people.
>
> *John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism*
>
> *July 2009*

***<u>Goal 4 - Resource and Measure</u>: Ensure Components and Offices support and sustain the capacity and capability to share and safeguard mission-essential information throughout the HSE producing measurable results.***

***Objective 4.1 - Develop, Resource, and Deliver Operational Capabilities:*** Facilitate the development, resourcing, and delivery of operational capabilities and capacities for information sharing and safeguarding that maximize and support the current wide span of HSE partnerships.

***Key Objective Elements***

*4.1.1. Align, and where possible integrate, with other Departmental governance bodies leveraging collective demand to obtain and provide the necessary resources and investments to achieve effective sharing and safeguarding*

*4.1.2. Ensure Departmental resources and investments are continually meeting operational needs*

***Objective 4.2 - Streamline Sharing and Safeguarding Efforts:*** Continually review planned acquisitions and ongoing efforts to eliminate ineffective efforts and ensure compliance with national and DHS standards to optimize mission effectiveness through shared services and interoperability.

***Key Objective Elements***

*4.2.1. The ISSGB will work with the OCIO to establish and manage the Department's information sharing and safeguarding portfolio*

- Follow a disciplined process to assess the costs, benefits, and risks of potential information sharing and safeguarding product alternatives to streamline sharing and safeguarding efforts.
- Integrate assessment and determination of mission needs with available resources to allocate resources, manage risk, and optimize the fulfillment of the requirements across DHS's Planning, Programming, Budgeting, and Execution (PPBE) budget cycles.[28]
- Align investments and initiatives with the Department's goals and objectives maximizing return on investment.
- Implement the recommendations and activities of the Federal IT Shared Services Strategy among appropriate stakeholders to facilitate adoption of shared services.

*4.2.2. Work with the OCIO to ensure that sharing and safeguarding efforts comply with the ISSA*

- Improve assured network interoperability to best support enterprise-wide decision-making, reduce costs, and further promote the sharing of information and services between personnel, systems, and networks.

[28] DHS Directive 1330, *Planning, Programming, Budgeting, and Execution*, Feb 14, 2005 ("PPBE is the means by which the Department develops its Future Years Homeland Security Program (FYHSP) and associated five-year program resource requirements. It also guides development of the Department's budget request and establishes parameters and guidelines for implementing and executing the current budget").

*4.2.3. Collect and publish data on the annual and long-term funding the Department budgets and spends on sharing and safeguarding programs and activities*

- The ability for DHS to generate reliable cost estimates will lower the risk to the public and minimize overruns, missed deadlines, and performance shortfalls. Cost estimates will also allow decision-makers to prioritize future investments and demonstrate a continued commitment to support the capability and capacity of HSE mission operators' sharing and safeguarding of information.

***Objective 4.3 - Institutionalize a System of Accountability that Demonstrates Measurable and Sustained Progress, Results, and Value:*** Establish an institutionalized system of accountability that will enable DHS to demonstrate the results of information sharing and safeguarding efforts and how they have supported our missions.

***Key Objective Elements***

*4.3.1. Regularly review progress toward achieving sharing and safeguarding outcomes and continuously improve by planning, executing, evaluating, and adjusting actions to achieve desired results*

- Management standards dictate establishing anticipated outcomes and related timeframes or milestones as a part of a plan to oversee implementation activities. The ISSGB, through the ISCC and ISRMC, shall regularly review the progress toward achieving their annually published sharing and safeguarding outcomes and use their ongoing monitoring of these activities to continuously improve their efforts and inform funding decisions across the Future Years Homeland Security Program.
- Support certification and conformance processes allowing DHS to validate and certify they are employing sharing and safeguarding standards appropriately and better enable standards-based acquisition to promote interoperable products and services.

*4.3.2. Publish the results information sharing and safeguarding efforts have achieved and how they have supported our missions*

- DHS must move towards establishing measures that better hold the Department accountable for our investments and expenditures.
- The ISSGB, through the ISCC and ISRMC, shall develop, institute, and report on outcome measures that determine the impacts that their sharing and safeguarding efforts have made on mission operators across the HSE. These measures may initially gauge stakeholders' satisfaction with timeliness, usefulness, and accuracy of information shared.

# V. Indicators and Measures

A number of existing laws require organizations to employ indicators and measures as a part of a performance measurement program to hold Departments and Agencies accountable to deliver results. *GPRA* and *GPRAMA* established statutory frameworks for performance management and accountability within the federal government. Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) and the Federal Information Security Management Act (FISMA) provide additional information sharing and safeguarding requirements. Based on these requirements and best practices, the ISSGB governance structure will develop and use indicators and measures that (1) assess accomplishments, (2) facilitate decision making, (3) hold DHS leaders accountable, (4) allow the HSE to continuously improve, and (5) provide more confidence to our stakeholders that the implementation of the *Strategy* is delivering results.

*GPRA* and *GPRAMA*, as well as the Government Accountability Office (GAO) and the National Institute of Standards and Technology (NIST), offer a variety of measurement categories applicable to sharing and safeguarding.[29] The typical accepted areas of measurement are either efficiency or effectiveness measures.[30] DHS indicators and measures shall have the following four key attributes:[31]

1. **Measurable:** Expressed in quantifiable values.
2. **Meaningful:** Measures are meaningful when they:
    a. Possess targets or thresholds for each measure to track progress over time;
    b. Define precisely what is being measured; and
    c. Link to organizational priorities, such as quality, timeliness, or best use of available resources.
3. **Repeatable and Consistent:** Defensible, auditable, use readily obtainable data, and could be easily reproduced.
4. **Actionable:** Support the decision-making and drive the behavior of those who are responsible for the control activities reflected in the measures.

[29] *See* GPRA and GPRAMA; GAO-09-617, *Information Security: Concerted Effort Needed to Improve Federal Performance Measures*, Sep 2009; NIST Special Publication 800-55, *Performance Measurement Guide for Information Security*, July 2008.

[30] "Efficiency measures" are defined as "input measures" (what an agency or manager has available (e.g., resources) to carry out the program or activity) or "process measures" (the opportunities for efficiency improvements identified between the transfer of inputs into outputs). "Effectiveness measures" are defined as "output measures" (the tabulation, calculation, or recording of activity or effort and can be expressed in a quantitative manner), "outcome measures" (the assessment of the results of an activity compared to its intended purpose), or "impact measures" (the direct or indirect effects or consequences resulting from achieving program goals). "Implementation/compliance measures" determine the extent to which stakeholders have adhered to mandated policies, regulations, etc.

[31] *See* GAO-09-617 at 9-12; *see also* GAO-12-137, *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements*, October 2011.

While using all types of measures is important to assess performance fully, DHS has shied away from utilizing "outcome" and "impact" measures. The DHS ISE has reached a level of maturity where it must develop measures that demonstrate the results that sharing and safeguarding efforts have achieved. Listed below is some guidance for the ISSGB and its members to develop indicators and measures.

> A key action and outcome for DHS is to evolve from a set of metrics that measures outputs, such as the number of intelligence reports issued, to an interim set that measures results, such as customer feedback on the quality of information shared, and finally, to the extent possible, to a set that measures homeland security outcomes achieved with the information sharing.
>
> *GAO Commissioner Dodaro, Letter to Secretary Napolitano, 29 September 2010*

1. ***Efficiency Measures***
   - **Process Indicators** - Develop appropriate measures that use quality, cycle time, and cost as important indicators of internal process performance.
2. ***Effectiveness Measures***
   - **Outcome Indicators** - Conduct independent evaluations to determine whether federal and nonfederal customers receive DHS information that is timely, accurate, trusted, and useful; meets their needs; and contributes to securing the Homeland.
     - Establish a baseline level of "satisfaction" (defined as timely, accurate, trusted, and useful information);
     - Set annual targets for improvement;
     - Track, measure, and report progress; and
     - Ensure findings from stakeholder feedback and performance evaluations lead to corrective action where appropriate.
   - **Impact Indicators**
     - **Mission:** Develop appropriate measures that assess the direct and/or indirect effects or consequences resulting from the goals based on the *QHSR* missions.
       1. Impact of preventing terrorism and enhancing security;
       2. Impact of securing and managing our borders;
       3. Impact of enforcing and administering our immigration laws;
       4. Impact of safeguarding and securing cyberspace;
       5. Impact of ensuring resilience to disasters; and
       6. Maturing and Strengthening the Homeland Security Enterprise.
     - **Management:** Develop appropriate measures that assess the degree of budget and outcome alignment, and calculate the cost of achieving outcomes and target levels of performance.
3. ***Implementation/Compliance Measures:*** Develop appropriate measures that enable leadership to gauge the HSE's adherence to mandated policies, regulations, and applicable guidance.

The ISSGB shall apply this guidance to develop and implement a DHS sharing and safeguarding performance management program. This program and the development of indicators and measures *must* be a fundamental and crucial part of the forthcoming Information Sharing and Safeguarding Action Plan *(see, infra, Section IX - Way Ahead: Develop and Implement an Action Plan).*

# VI. Alignment with the *National Strategy for Information Sharing and Safeguarding*

Section 1016 of the IRTPA, as amended, called for the establishment of an Information Sharing Environment (Federal ISE) "for the sharing of terrorism information…consistent with national security and…with applicable legal standards relating to privacy and civil liberties."[32] The *2007 National Strategy for Information Sharing* reinforced the importance of information sharing as a national priority. It also integrated all prior terrorism-related information sharing policies, directives, plans, and recommendations and provides a national framework against which to implement the ISE.

DHS has been an active participant in the Federal ISE since its inception through furthering the Federal ISE goals, evidenced in the PM-ISE's *2007-2012 Annual Reports to Congress*, and leading initiatives arising out of the Information Sharing and Access Interagency Policy Committee (ISA IPC) and its Sub-Committees.[33]

With the 2012 publication of the *National Strategy for Information Sharing and Safeguarding*, the White House and the PM-ISE builds on the *NSIS*. During the development of this *Strategy*, DHS has worked closely with the White House National Security Staff as well as the PM-ISE ensuring our planned efforts align to the updated NSISS. Our continued active participation in the ISA IPC and Sub-Committees will permit DHS to play its crucial role in enhancing national and homeland security.

[32] IRTPA, as amended, §1016(b)(1)(A). The scope of the ISE was originally limited to "terrorism information" as defined in Section 1016. In August 2007, the *Implementing Recommendations of the 9/11 Commission Act of 2007* (P.L. 110-53), included amendments to Section 1016 that expanded the scope of the ISE to explicitly include homeland security and weapons of mass destruction information and identified additional ISE attributes. It also endorsed and formalized many of the recommendations developed in response to the Presidential information sharing guidelines, such as the creation of the Interagency Threat Assessment and Coordination Group, and the development of a national network of state and major urban area fusion centers.

[33] The White House established the ISA IPC in 2009. It subsumed the role of a predecessor interagency body (the Information Sharing Council) established by Section 1016 of IRTPA. The White House's Senior Director for Information Sharing Policy and the PM-ISE co-chair the ISA-IPC.

| | DHS Capstones | | | | | DHS Goals | | | |
|---|---|---|---|---|---|---|---|---|---|
| ***DHS Strategy* Capstones and Goals** / ***National Strategy* Goals** | **1. Manage Information as a National Asset** | **2. Embrace a Risk-Informed Culture** | **3. Protecting Privacy, Civil Rights, And Civil Liberties is Paramount** | **4. Develop and Implement Training, Incentives, and Tool** | **5. Commitment to Action** | **1. Share** | **2. Safeguard** | **3. Manage and Govern Risk** | **4. Resource and Measure** |
| 1. *Drive Collective Action through Collaboration and Accountability* | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 2. *Improve Information Discovery and Access through Common Standards* | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ |
| 3. *Optimize Mission Effectiveness through Shared Services and Interoperability* | ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| 4. *Strengthen Information Safeguarding through Structural Reform, Policy, and Technical Solutions* | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 5. *Protect Personally Identifiable Information, Privacy, and Civil Liberties through Consistency and Compliance* | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

**Table 1: *National* and *DHS Strategies* Alignment Matrix**

# VII. Way Ahead: Publish an Implementation Plan in 90 Days

This *Strategy* establishes the Department's vision, mission, capstones, goals, and objectives and provides guidance to develop indicators and measures as a basis to hold ourselves accountable to deliver quantifiable results for mission operators across the HSE. DHS recognizes that to enable the missions of the HSE, it will have to develop an implementation plan.

The ISSGB shall publish an implementation plan within 90 days of this *Strategy*'s issuance date. The purpose of the implementation plan is to: (1) provide a useful tool for the ISSGB in guiding, measuring, and tracking progress toward achieving the *Strategy*'s vision, goals and

objectives; (2) identify initiatives that address gaps in capabilities that, if completed, will represent achieving the objectives; and (3) identify who is accountable to deliver what, by when, and the desired outcome of each initiative. It is paramount that the initiatives included in the implementation plan enable mission operators to do their jobs better.

Once the ISSGB publishes the implementation plan, it shall use its Sharing and Safeguarding Roadmap (Roadmap) to monitor progress toward achieving the plan's related milestones, deliverables, and resources, and by reference, the *Strategy*'s vision, goals, and objectives. The ISSGB, through the ISCC, ISRMC, and/or ESCs, shall also use the indicators and measures developed through its performance management efforts to demonstrate mission outcomes. The ISSGB shall publish the progress toward achieving the plan (e.g., Roadmap) and the results of its measurement program no less than quarterly to the ISSGB and its members and include this information in the ISSGB's Annual Report.[34]

[34] *See ISSGB Charter*, Responsibility "H," November 2011.

# VIII. Appendix A: Key Mandates and Reference Documents

**Statutory/Executive**

- Homeland Security Act of 2002, Sections 201 and 892
- Intelligence Reform and Terrorism Prevention Act, Section 1016 (as amended)
- Implementing the 9/11 Commission Recommendations Act of 2007 (Title 5)
- Executive Orders 12333, 13356, 13388, and 13587
- White House Memoranda, *Memorandum to the Heads of Executive Departments and Agencies on the Guidelines and Requirements in Support of the Information Sharing Environment*, 16 December 2005
- White House Memoranda on Strengthening Information Sharing and Access, July 2009
- Presidential Policy Directive 8, *National Preparedness*, 30 March 2011
- *National Strategy for Information Sharing*, October 2007
- *National Strategy for Information Sharing and Safeguarding*, 2012

**GAO Reports and Related DHS Commitments**

- GAO, *Information Sharing: Progress Made and Challenges Remaining in Sharing Terrorism-Related Information*, GAO-12-144T, October 2011
- GAO, *Department of Homeland Security - Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11*, GAO-11-881, September 2011
- GAO, *Information Sharing Environment: Better Roadmap Needed to Guide Implementation and Investments*, GAO-11-455, July 2011
- GAO, *Information Sharing: DHS Could Better Define How It Plans to Meet Its State and Local Mission and Improve Performance Accountability*, GAO-11-223, December 2010
- GAO, *Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results*, GAO-10-972, September 2010
- *DHS I&A, DHS Information Sharing Corrective Action Plan and Addendum (submitted to GAO)*, October and December 2010
- *GAO Commissioner Dodaro Letter to DHS Secretary Napolitano*, 29 September 2010
- GAO, *Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results*, GAO-10-972, September 2010
- GAO, *Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, GAO-08-492, June 2008
- GAO, *Homeland Security: Federal Efforts Are Helping to Address Some Challenges Faced by State and Local Fusion Centers*, GAO-08-636T, April 2008

**DHS Strategies/Policies**

- *US Department of Homeland Security Strategic Plan for FY 2012-2016*, February 2012
- *Quadrennial Homeland Security Review*, February 2010
- DHS Delegation, "Delegation to the Under Secretary for Intelligence and Analysis/Chief Intelligence Officer," *DHS Delegation No. 08503*, August 10, 2012

- *DHS Policy for Internal Information Exchange and Sharing*, February 2008
- *Memorandum on Implementation of One DHS Information Sharing Memorandum* ("One DHS Memo"), February 2007
- Intelligence Community Directive 501, January 2009
- *Memorandum on Inclusion of Information Sharing Competencies in Performance Appraisals*, July 2009
- Memorandum on Designation of Information Sharing and Knowledge Management Officers, March 2009

**DHS Governance**

- Information Sharing and Safeguarding Governance Board Charter, October 2011
- Information Sharing Coordinating Council Charter, September 2009
- Information Safeguarding and Risk Management Council, October 2011

U. S. Department of Homeland Security