National Infrastructure Advisory Council

Implementation of EO 13636 and PPD-21

DRAFT Report and Recommendations

November 5, 2013

David Kepler
Working Group Co-Chair
Chief Sustainability Officer,
Chief Information Officer
The Dow Chemical Co.

Philip Heasley
Working Group Co-Chair
President and CEO
ACI Worldwide

About the NIAC

The National Infrastructure Advisory Council (NIAC) advises the President of the United States through the Secretary of Homeland Security on issues related to the security and resilience of the Nation's critical infrastructure sectors and their functional systems, physical assets, and cyber networks for the 16 critical infrastructure sectors. These critical infrastructure sectors span the U.S. economy and include the chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems sectors. The NIAC also advises the lead Federal agencies that have critical infrastructure responsibilities. Specifically, the Council has been charged with making recommendations to:

- Enhance the partnership between the public and private sectors in securing and enhancing the security and resilience of critical infrastructure and their functional systems, physical assets and cyber networks, and providing reports on this issue to the President through the Secretary of Homeland Security, as appropriate;
- Propose and develop ways to encourage private industry to perform periodic risk assessments and implement risk reduction programs;
- Monitor the development and operations of critical infrastructure sector coordinating councils and their information sharing mechanisms and provide recommendations to the President through the Secretary of Homeland Security on how these organizations can best foster improved cooperation among the sectors, the Department of Homeland Security (DHS), and other Federal Government entities;
- Report to the President through the Secretary of Homeland Security who shall ensure appropriate coordination with the Assistant to the President for Homeland Security and Counterterrorism, the Assistant to the President for Economic Policy, and the Assistant to the President for National Security Affairs; and,
- Advise sector specific agencies with critical infrastructure responsibilities, to include issues pertaining to sector and government coordinating councils and their information sharing mechanisms.

Table of Contents

1. Introduction

The protection of the country's critical infrastructure security and resilience can be most effectively advanced by continuing to strengthen the collaboration between the public and the private sectors. This collaboration should be focused on the desired outcome of mitigating the impact of threats and attacks. For cyber threats, this should be based on a risk- and performance-based approach, managing the relationship to physical security, continuing to improve two-way information sharing, prosecution of cyber criminals and protection of the information that is shared from unintended use. This can be done in a way that builds on the cooperative relationships developed over the past decade between the public and private sectors.

This document provides feedback and comments on the body of work that has emerged from the engagement of private sector owners and operators in the implementation of Executive Order (EO) 13636 and Presidential Policy Directive 21 (PPD-21), as well as the update to the National Infrastructure Protection Plan (NIPP).

On February 12, 2013, the President signed EO 13636 and PPD-21, effecting changes throughout the critical infrastructure security and resilience (CISR) mission. The two documents were released concurrently in order to allow for a comprehensive approach to security and risk management, as well as to link cyber resilience and security to physical asset security and resilience.

Goals of EO 13636 included the development of a voluntary cybersecurity network; encouraging the adoption of enhanced cybersecurity practices through promotion and incentives; increasing the volume, timeliness, and quality of information sharing; ensuring privacy and civil liberties are protected with regard to enhanced cybersecurity; and exploring existing cybersecurity regulations for possible inclusion in the framework. PPD-21 — which replaces Homeland Security Presidential Directive 7 — requires the development of near-real-time situational awareness of the status of physical and cyber infrastructure assets; exploration of the cascading impacts of critical infrastructure failures; evaluation of how to further develop the partnership between all levels of government and private sector owners and operators; the development of a comprehensive research and development plan; and the updating of the NIPP.

On April 8, 2013, the Administration directed the Council to study and offer recommendations on the implementation of the EO 13636 and PPD-21 in the critical infrastructure security and resilience (CISR) mission.

The Council was asked to address three primary issues in this study: the revision of the NIPP, the enhancement of information sharing between government and the private sector, and the development of the voluntary cybersecurity framework. With regard to the NIPP revision, Council members reviewed drafts of the plan throughout the development and revision process, provided comments on the initiatives laid out in the plan, and considered methods for increasing adoption of the plan in the private sector. The NIAC's review of information sharing sought to address issues such as effective mechanisms for sharing, principles to encourage greater collaboration, and how to measure the success of efforts to

increase information sharing. In its review of the voluntary cybersecurity framework, the Council considered the scope and priorities of the framework, areas for further consideration and improvement, and methods and incentives for encouraging maximum adoption of the framework by private sector owners and operators.

Having national unity of effort to strengthen and maintain a secure, functioning and resilient infrastructure requires broad participation, collaboration and trust. The probability of success will be improved by incorporating the key principles and outcome-based deliverables explained in this document in all aspects of EO 13636, PPD-21, and the updated national plan.

The NIAC presented its preliminary findings and recommendations over the course of three public meetings held between July and September, 2013. The July meeting addressed the Council's preliminary analysis and findings on the revised NIPP and potential incentives for the adoption of the cybersecurity framework. In the August meeting, Council members discussed information sharing recommendations developed in response to framing questions submitted by the Administration. The final public meeting, held in September, focused on the Council's findings and recommendations on the cybersecurity framework, metrics for determining the efficacy of the framework, and how to encourage maximum adoption by private sector owners and operators.

2. Framework for Recommendations

In development of its final report, the NIAC addressed a series of questions covering the material being produced in reference to EO 13636 and PPD-21.

Incentives for Adopting the Cybersecurity Framework

Successful implementation of the voluntary cybersecurity framework is reliant on widespread buy-in from private sector owners and operators, and incentives are a key component of generating interest and participation. The Administration offered several potential incentives that could assist in encouraging adoption of the voluntary cybersecurity framework. Proposed incentives included:

- Expedited Security Clearance Process
- Grants
- Include Cybersecurity in Rate Base
- Information Sharing
- Insurance
- Liability Considerations
- New Regulation/Legislation
- Prioritized Technical Assistance
- Procurement Considerations
- Public Recognition
- Security Disclosure
- Streamline Information Security Regulations
- Subsidies
- Tax Incentives

The NIAC was asked to review these options, determine the relative value and the likelihood of adoption of each incentive, and to suggest any additional incentives that would encourage greater participation. The complete list of scoping questions can be found in Appendix A.

Information Sharing

Following the review of incentives, the NIAC was asked to consider information sharing, and the successes and challenges of the current public-private information sharing environment. The Council addressed the following questions in its review:

> 1. What obstacles are there in the current information sharing environment with the Federal government and with the State, local, tribal, and territorial (SLTT) governments? What do your employees see when they try to obtain or send information to the Federal government? What causes the greatest challenges and inefficiencies that demotivate sharing of information with the Federal government or with SLTT governments?

2. What are incentives to increased information exchange?

3. What are the most effective mechanisms/processes?

4. What are the unique aspects of cyber information sharing that might differ from physical information sharing? Is the right information reaching the right people to take the action that is needed? If not, what is the best way to address this challenge, specifically with regard to cyber information sharing?

5. What principles or actions that can be taken will be most likely to encourage voluntary information sharing? Which will be least likely to encourage adoption?

6. What is the core value proposition for cyber-related information sharing (two-way?)

7. How should the Federal Government and private sector owners and operators track metrics for timely and coordinated sharing of cyber threat information and situational awareness at appropriate classifications? What might be the metrics for effective information sharing in both cyber and physical/operational dimensions?

Cybersecurity Framework

The NIAC was asked to review the elements of the proposed cybersecurity framework. The Administration asked that the Council determine the aspects of the framework most likely to be beneficial to private sector owners and operators, as well as how the Federal Government can facilitate the adoption of the program. Framing questions included:

1. What necessary elements must be in the Framework in order to facilitate broadest adoption by owners and operators?

2. What might be the most efficient and effective processes facilitating adoption? What can the Government can do to facilitate?

3. What is the best way for the government to measure usefulness and adoption of the framework?

4. What obstacles prevent adoption, particularly for those organizations beyond the Fortune 1000?

5. What audience(s) should be targeted to facilitate adoption?

6. What issues exist that require alignment across Federal agencies, regulatory and non-regulatory, and with other levels of government? How should these issues be addressed?

NIPP Revision

Council members were also asked to review drafts of the revised NIPP, and then offer comments and recommendations on the national plan's initiatives and policies. In addition, the Council was asked to consider methods of encouraging wider adoption of the NIPP by owners and operators.

Members were asked address the following concepts:

1. How does the Federal Government write a short and clear revised plan that is flexible, adaptable, and readable to owners and operators outside of the Beltway?

2. What has to be in the plan for it to be seen as useful and applicable to owners and operators?

3. How do we incorporate the concepts of how the critical infrastructure mission can operate in a "networked-coordination" environment; but provide enough structure and order that those who are going to be implementing the NIPP can build their own plans, processes, etc.in a measurable way from a national perspective?

4. How can the plan focus on critical functions and services — such as the lifeline infrastructures and dependencies by the other sectors — while maintaining appropriate and relevant risk-based momentum in the other sectors?

5. How can the plan incorporate appropriate support for the wider estimated 4.8 million-strong owner-operator community, so they also can benefit from the national programs, capabilities, and lessons learned; where to go for infrastructure security and resilience information; and advice and guidance (given continued restrained Federal resources)?

3. Findings and Conclusions

The work on the implementation of EO 13636, PPD-21, the revision to the NIPP, and the creation of the voluntary cybersecurity framework, can be best aligned by ensuring three fundamental questions are addressed:

1. What is the Critical Purpose?
2. How will achieving this purpose be measured?
3. What will incentivize effective collaboration between the public and private sectors to address the Critical Purpose?

CRITICAL PURPOSE: National and Economic Security from National Threats, Including Cyber

For cyber threats, the Critical Purpose is clearly outlined by the President in EO 13636:

> "Repeated cyber intrusions into critical infrastructure demonstrate the need for improved Cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats."

This NIAC working group agrees with the President's sense of urgency. The development and implementation of EO 13636 and PPD-21 — including the framework, their structure, processes and participation — must be based on this critical outcome.

Adopting the Cybersecurity Framework

Finding 1: The key factor to encourage adoption by the private sector of the Cybersecurity Framework is creating confidence that it is effective in securing the nation from cybersecurity threats

Finding 2: The incentives most likely to encourage confidence and participation of critical infrastructure owners and operators are: an effective framework, good-faith protection of shared information, streamlining of regulations, and outcome-based metrics.

2.1 An effective framework improves security posture in a cost-effective manner, and would include:

a. Clear outcome-focused objectives and goals in securing critical infrastructure assets
b. Transparency and focus on high-priority threats
c. Clear and effective plans for the implementation of the national Cyber Security Program and framework

2.2 Information shared in order to address cybersecurity should be used for security purposes only. Companies acting in good faith are offered limited protection from subsequent liability and antitrust issues, as well as review by other government agencies regarding that information.

2.3 Existing regulations should be reviewed, in order to streamline complex rules and to remove duplicative instances. The cybersecurity risk framework should be developed to leverage or give credit for compliance with existing regulations (SoX, HIPAA, CFATS, etc.) and avoid duplication of effort, including elimination of compliance with multiple standards.

2.4 The use of clear, outcome-based metrics will help to improve these requirements.

Finding 3: Focus on Purpose - Implementation will be better served by focusing on the Critical Purpose and related outcomes, such as goals and metrics, that allow the private sector to continue to implement effective cybersecurity systems, while expanding the public-private partnership.

There are successful examples in the industry of effective systems, such as the Department of Labor, Occupational Safety and Health Administration's (OSHA) Voluntary Protection Program (VPP) or the Department of Homeland Security's Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002. Similar processes could be enacted for cybersecurity, which would provide proactive risk management reviews of participating organizations. Those organizations that are certified as effectively managing risks would be given incentives in terms of reducing overlapping regulations and inspections or offering liability protections.

Information Sharing

At a high level, the framework on information sharing is aligned with the private sector's need for sharing timely and actionable information. This program can benefit all critical infrastructure sectors.

A significant challenge is to share information in a timely, specific, and actionable way between the Government and private sector.

Finding 4: Creation of a Safe Harbor - with limited antitrust protection — that ensures information is used for intended purposes only, and offers protection from liability when acting in good faith will encourage participation in the Information Sharing program.

Finding 5: Information - The opportunity to receive timely, actionable information is the most significant incentive in encouraging companies to participate in the information sharing program.

Additional incentives could include technical guidelines, support and sharing of cyber security practices between DHS/NSA and the private sector. In addition access to indicators via a portal similar to those used in HSIN and US CERT would be of value to the private sector.

Information should be in a format and specificity that can be used by each company to search their own security logs (i.e. IP addresses, domains, malware hashes, etc.). Sharing specific vulnerabilities, threats, methods and motivations of attackers will also help private sector owners and operators make more accurate and effective use of resources to improve cybersecurity postures.

All current Federal mechanisms for Information Sharing (including — but not limited to — one-on-one, ISACs, US-CERT, and intelligence briefings) should be reviewed with the goal of simplifying processes, eliminating redundancy, improving coordination among different Federal agencies and ensuring consistency of information delivered as suggested by NIAC in 2012.

DHS should collaborate with the private sector on information sharing work process definition, to ensure that procedures are effective and efficient for exchanging information between owners and operators and government at all levels.

Finding 6: Classification of Information - Over-classification of information is a significant barrier to effective information sharing programs.

Information needs to be more finely divided, so that as much of what is shared as possible can be declassified. That will allow more information to be disseminated among the private sector to resources that can take specific actions.

Although DHS plans to expedite clearances, there needs to be more clarity on how classified information can be used within a company whose monitoring systems will not be certified for classified information. If action is to be taken, information needs to be declassified for deeper and broader communication within a company or industry. CISOs and CIOs are not solely responsible for the execution of cybersecurity. Unlike some information that could be actionable despite being highly compartmentalized, the use and implementation of Information Technology systems and controls crosses entire facilities and organizations. As a result, there is a need for cybersecurity information to be disseminated more broadly.

Finding 7: Intended Use - The private sector is concerned that the sharing of some forms of information could lead to governmental inquiries and regulation beyond the original purpose for which the information was offered.

To allay such concerns, and in appreciation of the greater benefits that may arise from encouraged information sharing by the private sector to the public authorities, the Federal Government could, for example, provide mechanisms to assure that information will remain confidential and not disseminated within the government except where there are legitimate and compelling reasons to do so. To further illustrate, such mechanisms might range from the designation of particular means and channels of communication to assure confidentiality, to the creation of “safe harbors” whereby private sector

entities could have limited antitrust protection, the ability to divulge information free of civil or criminal liability under privacy protection laws, and to the establishment of exceptions for disclosure regarding cyber incidents by SEC public reporting companies under limited conditions.

The DHS Protected Critical Infrastructure Information (PCII) program is a good example of a format that can be leveraged in all sectors to address this concern.

Finding 8: Information for Critical Purpose - As stated in the National Infrastructure Protection Plan, information sharing is a means to an end, not an end itself.

An information sharing effort should recognize, understand, and concur with a common goal. The Homeland Security Studies and Analysis Institute (HSSAI), a nonprofit, federally funded research and development center operated by Analytic Services Inc. on behalf of DHS, has created document titled "Metrics for Measuring the Efficacy of Critical Infrastructure-Centric Cybersecurity Information Sharing Efforts." (see Appendix B) This document details options for metrics that include the attributes of effective information sharing (such as relevance, timeliness, and accuracy) and the outcome-based goal of information sharing, which is primarily "no loss of control." We recommend that this document serve as the framework for the development of the metrics.

Cybersecurity Framework

The cybersecurity framework presents a coherent approach to crafting an effective cybersecurity program based on established standards and practices.

The Council observed several valuable aspects of the proposed cybersecurity framework, including:

1. Care has been taken throughout the development process to stress that use of the framework is voluntary
2. The Function, Category and Subcategory hierarchy has been used in the framework core. That hierarchy is similar to those included in Quality Management Systems plans, and allows for flexibility in application. The concept of "tiers" is similar to levels typically seen in IT Industry capability maturity models.
3. There is specific and actionable guidance on how to apply the framework, including practical examples.
4. Partnership between government and private sector owners and operators is emphasized, not only in the development of the framework, but in its continued application.
5. A risk-based approach is used, acknowledging that there are differences by industry or sector, and that cyber risk management should be integrated with existing processes, and is not something separate.

Finding 9: Metrics - Metrics and milestones that measure outcomes will be key to the success of the cybersecurity framework.

The key principles for the success of the cybersecurity framework must include:

9.1 Focusing first on securing the lifeline sectors (Energy, Water, Transportation, and Telecommunications) and their interdependencies.

9.2 Engaging participation of the Information Technology (IT) Sector in the recognition that improving quality and security of IT products and services are required to protect the cyber backbone of the lifeline sectors. Government agencies and the financial sector — and their networks — are foundational to these lifeline sectors, and will also need a high-priority focus.

9.3 Using an outcome-based process in identifying significant risks and methods for mitigating those risks, including response preparedness.

9.4 Sharing of relevant and actionable information between the Government and private sector owners and operators, with adequate protection to ensure the information is used only for the Critical Purpose.

9.5 Leveraging and aligning existing standards, management systems and regulations that are demonstrated to work toward achieving the Critical Purpose.

9.6 Pursuing and prosecuting those participating in cyber criminal and espionage acts.

Finding 10: Evergreen Process - An ongoing effort will be required in order to gain the most value from the cybersecurity framework.

Specific areas for further consideration or improvement should include:

10.1 A focus on both process- and outcome-based metrics as a means of assessing effectiveness in applying the Framework. See Figure 1 below as an example of metrics that can be used to assess effectiveness of the whole national cybersecurity program, including the cybersecurity framework. This attachment is included in the document "Metrics for Measuring the Efficacy of Critical Infrastructure Cybersecurity Information Sharing Efforts," by Fleming/Goldstein 2012 (see Appendix A).

10.2 More specifics are needed with respect to who will own and be responsible for the continued development of this framework after it is released. We agree with the stated goal for this to be in the private sector.

10.3 The framework should include sections on information sharing and benchmarking, to ensure that companies establish processes to gather cyber intelligence and to assess cyber programs versus industry trends and practices.

10.4 Detail about the mechanisms that will be used to improve and develop this model, and to coordinate its application for the purpose of sharing of experiences, need to be developed.

10.5 Additional basis for and emphasis on security standards for IT products is required, such as in the Secure by design concept. This is a critical foundational element of the framework. For industrial control systems, the ISA/IEC 62443 series addresses this specifically.

10.6 Given the focus on lifeline sectors (Energy, Water, Transportation and Telecommunications) and their interdependencies, more emphasis on Process Control Systems and the specific or unique characteristics or constraints is required (The private sector is continuing to address this through collaboration among the International Society of Automation (ISA), the Automation Federation and the developers of the framework). For example, the precedence of Confidentiality over Integrity and Availability that is typical for information systems changes to a preference for Availability and Integrity over Confidentiality for industrial systems design.

Table ES1. Metrics for Measuring the Performance of Critical–Infrastructure–Centric Cybersecurity Information Sharing

Inputs	Processes	Outputs	Outcomes
Shared information comprises both data and meaning: ▪ % of participating entities reporting that shared information received in a given time period contains both data and meaning ▪ % of submitted information and analytic products (based upon a random sample) that contain both data and meaning **Shared information is relevant:** ▪ % of participating entities reporting that the shared information they receive in a given time period informs decisions that reduce cyber risks to critical infrastructure ▪ % of participating entities reporting that the shared information they receive in a given time period contains new data, new meaning, or both ▪ % of *specific* information submissions or analytic products released in a given time period that inform decisions, and contain new data, new meaning, or both ▪ Number of instances in a given time period that *specific* submissions or products that were not yet known about led to the discovery of a previously unknown cyber incident, once deployed	**The goal is specified:** ▪ % of participating entities reporting that the goal has been developed, issued, and disseminated by a coordinating body **The goal is agreed upon:** ▪ % of participating entities providing express or implied concurrence with goal **Participating entities are appropriate:** ▪ % of participating entities who meet specified criteria ▪ % of participating entities who report that they can generate, analyze, or use information to achieve the goal **Entities are participating:** ▪ % of entities logging on to the information sharing website at least once in a given time period ▪ % of entities sending information to the website at least once in a given time period ▪ % of entities receiving information from the website at least once in a given time period ▪ % of entities participating in scheduled collaborative exchanges in a given time period ▪ % of entities with at least one person on the NCCIC floor at least once in a given time period ▪ % of entities who report independent collaboration with other entities in a given time period ▪ % of entities responding to RFIs in a given time period	**Information is used for tactical and strategic purposes:** ▪ % of participating entities reporting use of shared information to improve or implement security controls in a given time period (tactical use) ▪ % of participating entities reporting use of shared information to inform resource allocation decisions in a given time period (strategic use) ▪ % of received (i.e., accessed) information used to improve or implement security controls in a given time period (tactical use) ▪ % of received (i.e., accessed) information used to inform resource allocation decisions (strategic use)	**Goal is achieved** (all in a given time period): ▪ Number of incidents causing unavailability of critical services and estimated associated costs of damage ▪ Number of incidents causing the loss of critical data and estimated costs of damage ▪ Number of detected incidents, both prevented and successful, and estimated costs of damage ▪ Unplanned downtime ▪ Mean time to incident detection ▪ Mean time to incident remediation ▪ Mean time to incident recovery ▪ Mean time between failures

Figure 1

http://www.homelandsecurity.org/docs/reports/RP11-01.02.02-01_Final%20Report_31Mar12.pdf

NIPP Revision

The NIAC sees a number of positive attributes in the revised NIPP (or its replacement) approach. In addition, the Council noted several worthwhile elements in the plan, including the use of a risk management framework; the adoption of an approach focused on outcomes and metrics, as opposed to the traditional process-driven approach; the advocacy for a broader coalition of public, private, non-governmental, local, and regional entities; and the emphasis on information sharing and identifying the gaps in current information sharing initiatives.

Finding 11: Collaboration - The emphasis on promoting collaboration between governments and the private sector in development of the NIPP is particularly likely to increase the plan's chances of success.

Finding 12: Risk Prioritization — A risk management methodology is the right approach for determining the capabilities needed to enhance infrastructure security and resilience.

Sectors should be prioritized based on risk to human life, national commerce and homeland defense. All other sectors have significant interdependencies with the highest priority sectors such as Water, Energy, and Information Technology/Telecommunications.

Finding 13: Centralized Ownership — Housing of the Security Framework within an educational institution can help further develop the framework and promote the benefits of private sector adoption.

Successful examples of this type of development within the education sector can be found within Carnegie Mellon's Software Engineering Institute-CERT (Community Emergency Response Team) program.

4. Recommendations

Adopting the Cybersecurity Framework

The following are the Council's recommendations on incentives in addition to those that have been proposed by the Federal Government:

Recommendation 1: Limit liability on damages resulting from cybersecurity events.

Liability limits are an effective incentive to drive adoption of the cybersecurity framework by industry. However, the Council cautions against the creation of an environment where insurance underwriters are dictating security policies. Transferring risk to insurance companies does little to bolster security.

Recommendation 2: Use the Government's procurement power to encourage information technology suppliers to develop cybersecurity framework-compliant hardware and software.

Government procurement practices have numerous indirect benefits for the larger critical infrastructure community. It incentivizes suppliers to enhance the security of their products and services, which are often the same products and services used throughout the critical infrastructure security and resilience (CISR) community. Improvements to those systems and reducing the risk associated with hardware and software gaps also allow owners and operators to redirect their attention to other critical security concerns.

Recommendation 3: The Government should ensure the availability of qualified, vetted security professionals.

New areas of compliance require additional professionals to ensure compliance, and qualified personnel can be challenging to find. Federal assistance with background checks and leveraging of existing programs could establish a greater reserve of qualified professionals.

Recommendation 4: Grants, if used, should be focused on capacity building.

Direct Federal funding for investment should encourage adoption of the framework, through training, implementation, and more robust IT products, especially for small- to medium-sized operators. Any

contingencies placed on grants must be outcome-based and clearly articulated. Penalties for low success should not exceed the value of the grant.

Recommendation 5: "Metrics for Measuring of Efficacy of Critical Infrastructure Centric Cybersecurity Information Sharing Efforts," by Fleming/Goldstein 2012, should be leveraged in creating outcome metrics that can be used to measure the success of the EO and PPD implementation, including metrics such as indicators shared, attacks prevented, attackers caught, and risk mitigated.

Recommendation 6: The cybersecurity framework should be housed at a university, with base funding coming from critical infrastructure companies.

Engagement of small- to mid-sized owners and operators

While the work related to EO 13636 and PPD-21 is intended for use by owners and operators of all sizes, smaller operators may not have the resources or expertise to adequately leverage the tools that are in development.

Recommendation 7: The Federal Government should put forward additional effort to assist small- to mid-sized owners and operators in meeting the critical purpose outlined in EO 13636, in order to ensure reliable functioning of the Nation's critical infrastructure in the face of cyber threats, including:

Recommendation 7.1: Government-funded programs at universities to develop training to understand and best leverage the cybersecurity framework.

Recommendation 7.2: Government encouragement of IT providers and suppliers to create products that have security as a primary design criteria. Small to medium operators sometimes rely on off-the-shelf products that may not currently have adequate emphasis on security controls.

Recommendation 7.3: Government-developed training to assist small- and medium-sized owners and operators who lack resources or expertise.

Recommendation 7.4: Centralized ownership of the Security Framework within an educational institution to further develop the framework and promote the benefits of private sector

adoption. Successful examples of this type of development within the education sector can be found within Carnegie Mellon's Software Engineering Institute - Community Emergency Response Team (CERT) program.

Information Sharing

Recommendation 8: the Federal Government should adopt a policy that specifically addresses concerns that information sharing could lead to governmental inquiries and regulation beyond the original purpose for which the information was offered.

NIPP Revision

In reviewing the NIPP revisions, the NIAC sees areas for further review and refinement:

Recommendation 9.1: Security should be designed to be built in to systems, rather than layered on top of systems.

It is in this context that the Council believes that IT hardware/software providers should be part of the solution. It is their core IT products that must have security designed into them in order for critical infrastructure entities to be successful in protecting these systems.

Recommendation 9.2: The Government should leverage its purchasing power to incentivize enhanced security and resilience in core cybersecurity systems and programs (Information Technology, Industrial Automation, and Telecommunications sectors).

Recommendation 9.3: The Framework should include standards that address the risk management of Industrial Automation systems, which have unique control characteristics apart from general cybersecurity. Industrial Automation may warrant its own sector category.

Recommendation 9.4: The Government should develop policies and apply resources to pursue and discourage global cyber criminals from attacking critical infrastructure facilities.

Recommendation 9.5: The revised NIPP should include a summary specifically written for executives, in order to improve the understanding of the CISR mission.

Executive-level engagement is vital in any effort to encourage private sector use of the revised NIPP, and should be embraced in every public-private partnership activity.

The Federal Government should also pursue meetings with senior executive CEOs to further explain the relevance of the revised NIPP, and their role in it.

Recommendation 9.6: The Government should convene a public-private advisory panel under CIPAC to ensure that the needs of the private sector are addressed in the implementation of the revised NIPP.

5. Appendix A: Acknowledgements

EO-PPD Working Group Members

David Kepler (Co-Chair)
Executive Vice President,
Chief Sustainability Officer,
Chief Information Officer,
The Dow Chemical Company
Midland, MI

Philip Heasley (Co-Chair)
President and CEO,
ACI Worldwide
Elkhorn, NE

Constance H. Lau
President and Chief Executive Officer,
Hawaiian Electric Industries, Inc. (HEI)
Honolulu, HI

Glenn S. Gerstell
Managing Partner,
Milbank, Tweed, Hadley, & McCloy, LLP
Washington, DC

Michael J. Wallace
Senior Advisor and Director,
Nuclear Energy Program,
Center for Strategic and International Studies;
Former Vice Chairman and COO,
Constellation Energy
Washington, DC

6. Appendix B: Framing Questions on Incentives

PRESIDENTIAL POLICY DIRECTIVE 21 AND EXECUTIVE ORDER 13636
NIAC EO/PPD IMPLEMENTATION WORKING GROUP

INTEGRATED TASK FORCE INCENTIVES FOR VOLUNTARY ADOPTION

Framing Questions for Working Group Member Consideration:

1. What incentives are most likely to be adopted voluntarily by owners and operators?

2. What incentives are least likely to be adopted voluntarily by owners and operators?

3. Executive level engagement with the Federal government helps Executives create priorities, allocate resources, and hold individuals accountable for private sector actions. What steps can be taken to ensure Executives are engaged and driving voluntary incentive adoption?

4. Executives are cognizant of their fiduciary responsibilities to shareholders. How can the Federal government best reduce risk and uncertainty for Executives and encourage voluntary incentive adoption?

5. How can incentives best be paired with tools, technology, assets, and processes the government has, in order to encourage voluntary adoption?

6. How can Executive Summaries on incentive implementation be precisely and concisely written for Executives with little prior knowledge or experience in critical infrastructure security and resilience in order to communicate what happens, how things work, and how their risk and uncertainty are reduced?

7. How can the Federal government make all incentives voluntary while balancing regulation and oversight to facilitate a networked-coordination environment?

8. How can incentives best target lifeline sectors most critical in an actual emergency?

9. How can incentives best be prioritized to coordinate with infrastructures dependent on lifeline sectors that currently lack the resources, strength, or internal capabilities to bring themselves up to the level needed the case of an actual emergency?

10. What steps should be taken to ensure that all NIAC members are fully aware of the alignment and structure of all 16 sectors in order to prioritize incentives and their voluntary adoption?

11. To what extent should time limits and sunset clauses be incorporated to promote voluntary adoption?

12. Are there additional incentive categories that should be considered in addition to the 14 proposed?

13. Should any of the 14 proposed incentive categories be broken down further?

14. Is their relevant research, literature, or Member experience that the Working Group should consider in either cyber or non-cyber contexts?

7. Appendix C: Metrics

THIS SECTION INTENTIONALLY LEFT BLANK

Metrics for Measuring the Efficacy of Critical-Infrastructure-Centric Cybersecurity Information Sharing Efforts

Matthew H. Fleming, PhD, and Eric Goldstein[1]

15 November 2012

RP: 11-01.02.02-01

An FFRDC operated by Analytic Services Inc on behalf of DHS

[1] Fleming is a *Fellow*, Goldstein is an *Analyst*; both are with the Homeland Security Studies and Analysis Institute (HSSAI), a non-profit federally funded research and development center operated by Analytic Services Inc. on behalf of the U.S. Department of Homeland Security (DHS). Corresponding author's e-mail address: matthew.fleming@hsi.dhs.gov. Opinions expressed herein are those of the authors alone and represent neither those of HSSAI nor DHS. This document was approved for public release by the DHS Science and Technology Directorate on 15 November 2012.

Homeland Security Studies and Analysis Institute

The Homeland Security Act of 2002 (Section 305 of PL 107-296, as codified in 6 U.S.C. 185), herein referred to as the "Act," authorizes the Secretary of the Department of Homeland Security (DHS), acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. Analytic Services Inc. operates the HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE (HSSAI) as an FFRDC for DHS under contract HSHQDC-09-D-00003.

HSSAI provides the government with the necessary expertise to conduct: cross-cutting mission analysis, strategic studies and assessments, development of models that baseline current capabilities, development of simulations and technical evaluations to evaluate mission trade-offs, creation and evolution of high-level operational and system concepts, development of top-level system and operational requirements and performance metrics, operational analysis across the homeland security enterprise, and analytic support for operational testing evaluation in tandem with the government's acquisition process. HSSAI also works with and supports other federal, state, local, tribal, public and private sector organizations that make up the homeland security enterprise.

HSSAI research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under Task 11-01.02.02, "Cyber Security Information Sharing Metrics."

The results presented in this report do not necessarily reflect official DHS opinion or policy.

For information about this publication or other HSSAI research, contact:

HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE
Analytic Services Incorporated
2900 S. Quincy Street
Arlington, VA 22206
Tel (703) 416-3550
Fax (703) 416-3530
www.homelandsecurity.org

Contents

Abstract

Efforts to secure and defend public- and private-sector cyber systems rely in part on information sharing. Information sharing strengthens the nation's cybersecurity posture by allowing participating entities to have the broadest possible understanding of the tactics, techniques, and procedures of cyber threat actors and the vulnerabilities of cyber systems. Armed with this understanding, cyber defenders can better deter, prevent, disrupt, and recover from malicious cyber activity. Cybersecurity information sharing occurs in various fora in the public and private sectors. Within the Department of Homeland Security, the Office of Cybersecurity and Communications (CS&C) facilitates the sharing of actionable raw indicators and finished analytic products among entities in critical infrastructure sectors and the federal government. To ensure that such critical-infrastructure-centric cybersecurity information sharing efforts succeed in their missions, CS&C asked the Homeland Security Studies and Analysis Institute to develop a holistic, theory-driven suite of performance-measurement metrics. Taken together, metrics within this suite can serve to suggest whether efforts are 1) functioning as anticipated; and 2) having the desired impact. This paper presents the suite of metrics and associated findings of the research, including its theoretical foundations. Guided by first principles and literature on information, information theory, decision theory, and uncertainty (as well as best practices in performance measurement), the paper recommends using a suite of metrics that measure various relevant inputs, processes, outputs, and outcomes of critical-infrastructure-centric cybersecurity information sharing efforts.

Acknowledgements

The authors wish to thank Carlos Kizzee of DHS, as well as a large number of anonymous referees and contributors, including many private-sector cybersecurity information sharing partners. The authors also wish to thank Ryan Greer, Joseph Kendall, and Joseph Dunford for research assistance. Lastly, the authors are grateful to the many attendees of various conferences and open- and closed-door briefing sessions whose insightful questions and comments improved the content of this paper.

Acronyms

CIKR	Critical infrastructure/key resources
CISCP	(CIKR) Cyber Information Sharing and Collaboration Program (DHS)
CRADA	Cooperative research and development agreement
CS&C	Office of Cybersecurity and Communications
CSIS	Center for Strategic and International Studies
DCISE	DoD-Defense Industrial Base Collaborative Information Sharing Environment
DHS	Department of Homeland Security
DIB	Defense industrial base
DoD	Department of Defense
DSIE	Defense Secure Information Exchange
FBI	Federal Bureau of Investigation
FFRDC	Federally funded research and development center
FISMA	Federal Information Security Management Act of 2002
GAO	Government Accountability Office
GPRA	Government Performance and Results Act of 1993
HHS	Department of Health and Human Services
HSA	Homeland Security Act of 2002
HSPD	Homeland Security Presidential Directive
IDS	Intrusion detection system
IP	Internet protocol
IPS	Intrusion prevention system
ISA	Internet Security Alliance
ISAC	Information sharing and analysis center
ISP	Internet service provider
IT	Information technology
MSSP	Managed security service provider
NCCIC	National Cybersecurity and Communications Integration Center (DHS)
NCFTA	National Cyber Forensics and Training Alliance
NIAC	National Infrastructure Advisory Council
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NSIE	Network Security Information Exchange
NSPD	National Security Presidential Directive
ODNI	Office of the Director of National Intelligence
OIP	Office of Infrastructure Protection (DHS)
OMB	Office of Management and Budget
PCII	Protected critical infrastructure information
PDD	Presidential Decision Directive
PM-ISE	Program Manager-Information Sharing Environment
QHSR	Quadrennial Homeland Security Review
RFI	Request for information
SAR	Suspicious activity report(ing)
SSA	Sector specific agency
TSA	Transportation Security Administration (DHS)
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team (DHS)

I. Introduction

The Department of Homeland Security (DHS) has a central role to play in the cybersecurity of the United States. This role is summarized in the department's 2010 *Bottom-Up Review Report*, which notes that "by statute and Presidential directive, DHS has the lead for the Federal government to secure civilian government computer systems, works with industry to defend privately-owned and operated critical infrastructure, and works with State, local, tribal and territorial governments to secure their information systems" (DHS 2010a).

Efforts to secure and defend public- and private-sector systems rely in part on information sharing. Information sharing strengthens the nation's cybersecurity posture by allowing participating entities to have the broadest possible understanding of the tactics, techniques, and procedures of cyber threat actors and the vulnerabilities of cyber systems. Armed with this understanding, cyber defenders can better deter, prevent, disrupt, and recover from malicious cyber activity. For example, threat signatures, such as hostile internet protocol (IP) addresses, can be shared among entities and used in their intrusion detection and intrusion prevention systems (IDS/IPS).

Cybersecurity information sharing occurs in various fora in the public and private sectors. Within DHS, the Office of Cybersecurity and Communications (CS&C, part of the DHS National Protection and Programs Directorate) facilitates the sharing of actionable raw indicators and finished analytic products among entities in critical infrastructure sectors and the federal government.

To ensure that such critical-infrastructure-centric cybersecurity information sharing efforts succeed in their missions, CS&C asked the Homeland Security Studies and Analysis Institute (HSSAI) to develop a holistic, theory-driven suite of performance-measurement metrics. Taken together, metrics within this suite can serve to suggest whether efforts are 1) functioning as anticipated; and 2) having the desired impact.

This paper presents the suite of metrics and associated findings of the research. It is structured as follows: after this introduction, a background chapter provides context and sets forth the project's research question, methodology, and scope; a theoretical underpinnings chapter presents the foundations of performance measurement and information sharing upon which the metrics are built; a findings chapter recommends the suite of metrics; and a conclusion summarizes and closes with next steps and thoughts for future research.

II. Background

For context, this chapter provides an overview of cyberspace, cybersecurity, cybersecurity information sharing, critical infrastructure protection, and critical-infrastructure-centric cybersecurity information sharing efforts. It also presents the research question, methodology, and scope.

A. Cyberspace, Cybersecurity, and Cybersecurity Information Sharing

Cyberspace refers to "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people" (White House 2009, citing National Security Presidential Directive-54/Homeland Security Presidential Directive-23 [NSPD-54/HSPD-23]).

The United States relies on cyberspace in nearly all aspects of life. In sum, "the globally-interconnected digital information and communications infrastructure known as 'cyberspace' underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security" (White House 2009). Indeed, cyberspace underpins the bulk of U.S. critical infrastructure, including banking and finance, energy, communications, and transportation (on which more below).

Through cyberspace, malicious actors, accidents, and natural hazards can cause cyber and physical effects, such as the loss to competitors or adversaries of intellectual property; the loss of integrity of financial data; or, perhaps, the failure of part of the power grid.[2] Such effects result in physical, economic, and psychological costs to the nation, including (potentially) loss of life. Because of the U.S. reliance on cyberspace, these costs may be very significant.[3]

Cybersecurity and the activities that comprise it seek to minimize these costs. Cybersecurity activities include "the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure" (White House 2009).[4] Cybersecurity activities are carried out by public- and private-sector entities alike.[5]

---

[2] For useful background information on cybersecurity and the cyber threat, see Masters (2011). Also, malicious actors include state/nonstate actors, criminals, and "hacktivists"; accidents include software/hardware failures and human error; and natural hazards include things like earthquakes, hurricanes, floods, and tornadoes.

[3] At present, no agreed methods for measuring the costs of cyber incidents exist. Various estimates prevail in the literature, measuring various elements of the cybersecurity problem (some doing so more credibly than others). For example, a 2004 Congressional Research Service report estimated that the annual cost of malicious intrusions was $226 billion at that time (Cashell 2004). A 2010 white paper by the Internet Security Alliance (ISA) estimated that the cost to the nation of the theft of intellectual property was $1 trillion (ISA 2010). Some cyber incidents, not least those affecting critical infrastructure assets, may have more systemic second- and third-order effects, and thus incur potentially significant costs across sectors (see National Infrastructure Advisory Council [NIAC] 2007).

[4] Note that the quote, as it exists in the *Cyberspace Policy Review* (White House 2009), serves to define "cybersecurity policy"; it is used here to set forth a listing of cybersecurity activities. For a catalog of cybersecurity activities at the organizational level, see Special Publication 800-53 of the National Institute of Standards and Technology (NIST 2010) and also the "Twenty Critical Security Controls for Effective Cyber Defense" assembled by

Key among cybersecurity activities is cybersecurity information sharing, the topic of the present paper. In general, in cybersecurity information sharing, public- and private-sector cyber defenders share threat signatures, attack vectors, tactical vulnerabilities, and associated advice and context, either automatically or manually. Tactically, such information is used to better protect against threats, patch vulnerabilities, and mitigate incidents that may have occurred. For example, threat signatures are used to populate black-lists of various kinds, like those supporting antivirus software and IDS/IPS; signatures are automatically compared to inbound and outbound traffic, and are also used to search data at rest on local and network drives in order to detect and disrupt malware and malicious activity. Strategically, cybersecurity information sharing provides broad situational awareness to all involved, allowing for a common understanding of the nature of cyber threats and vulnerabilities and trends therein. Such understanding informs investment decisions and research agendas, among other things.

B. Critical Infrastructure Protection

Cybersecurity information sharing helps to secure and defend critical infrastructure. As noted above, critical infrastructure resides in sectors like banking and finance, energy, communications, and transportation.[6] Formally, "critical infrastructure" represents "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (USA PATRIOT Act of 2001 [42 U.S.C. 5195c Sec. 1016e]).[7]

---

the SANS Institute (SANS 2009). The *National Infrastructure Protection Plan* (*NIPP*; DHS 2009a) defines cybersecurity as follows: "The prevention of damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems and services (and the information contained therein) to ensure confidentiality, integrity, and availability."

[5] As noted, DHS plays a central role in securing and defending cyberspace. For information on the authorities supporting and governing this DHS role, see Fleming and Goldstein (2011).

[6] The *NIPP*, as per HSPD-7, categorizes critical infrastructure assets into 18 sectors, each led by a federal government sector specific agency (SSA). HSPD-7 originally identified 17 sectors; critical manufacturing was added later. Sectors are as follows (with SSAs listed in parentheses after each): agriculture and food (Department of Agriculture; Department of Health and Human Services [HHS]); defense industrial base (DoD); energy (Department of Energy); healthcare and public health (HHS); national monuments and icons (Department of the Interior); banking and finance (Department of the Treasury); water (Environmental Protection Agency); chemical (DHS Office of Infrastructure Protection [OIP]); commercial facilities (DHS OIP); critical manufacturing (DHS OIP); dams (DHS OIP); emergency services (DHS OIP); nuclear reactors, materials, and waste (DHS OIP); information technology (DHS Office of Cybersecurity and Communications); communications (DHS Office of Cybersecurity and Communications); postal and shipping (DHS Transportation Security Administration [TSA]); transportation systems (DHS TSA; United States Coast Guard); government facilities (DHS Immigration and Customs Enforcement; DHS Federal Protective Service). For more on critical infrastructure protection, see http://www.dhs.gov/files/programs/critical.shtm.

[7] This paper uses the term "assets" to refer to both "systems and assets" (including data, like those pertaining to intellectual property). Critical infrastructure is also sometimes referred to as "critical infrastructure/key resources" (CIKR), where "key resources" represent "publicly or privately controlled resources essential to the minimal operations of the economy and government" (Homeland Security Act of 2002 [HSA; 6 U.S.C. 101 Sec. 9]). Also, note that the 2011 DHS *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise* (DHS 2011a) identifies a concept it calls "critical information infrastructure," defined as: "Any physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any form

By definition, the United States relies on its critical infrastructure. Because of this, as noted in the *National Infrastructure Protection Plan* (*NIPP*), "attacks on CIKR [critical infrastructure/key resources; see footnote 7] could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident" (DHS 2009a). Damage to critical infrastructure—whether physical or cyber, malicious or accidental—is to be avoided.

Led by DHS, all parties in the public and private sectors have a role to play in efforts to protect critical infrastructure. The Homeland Security Act of 2002 (HSA) requires DHS to "recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities." HSPD-7 expands upon the HSA. Among other things, it codifies the role of DHS in "coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States." The national public-private approach to critical infrastructure protection is set forth in the *NIPP*, which was initially published in 2006 and revised in 2009.[8] The *NIPP* provides a "unifying structure for the integration of existing and future [critical infrastructure] protection efforts and resiliency strategies into a single national program" (DHS 2009a).

Guided by the *NIPP*, critical infrastructure is protected by identifying assets and assessing, prioritizing, and mitigating risks. This is inherently difficult, not least due to the existence of cyber and physical one-way dependencies, interdependencies, and cascading effects between assets.[9] That is, because of dependencies and interdependencies, failure of one critical infrastructure asset can lead to degraded performance or failure of another critical infrastructure asset. This implies that effective critical infrastructure protection requires an understanding of often nonobvious relationships; this understanding may be more difficult in the cyber domain, a point discussed later in the present paper.

---

including data, voice, or video that is: Vital to the functioning of critical infrastructure; so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on national security, national economic security, or national public health and safety; or owned or operated by or on behalf of a State, local, tribal, or territorial government entity." The *NIPP* (DHS 2009a) also defines cyber infrastructure: "Includes electronic information and communications systems and services and the information contained therein. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information."

[8] Drafting of the *NIPP* is required by the HSA, which calls for the department to "develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States."

[9] The *NIPP* (DHS 2009a) directly addresses the intersection of cybersecurity and critical infrastructure protection, noting that "cybersecurity includes preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability…the interconnected and interdependent nature of the Nation's [critical infrastructure] makes it problematic to address the protection of physical and cyber assets independently." The information technology sector specific plan (DHS 2010b) similarly addresses this consideration, noting in part that the "high degree of interdependency of the IT Sector, its interconnectedness, and non-traceable and unidentifiable actors makes identifying threats, assessing vulnerabilities, and estimating consequences difficult and must be dealt with in a collaborative and creative manner."

C. Critical-Infrastructure-Centric Cybersecurity Information Sharing Efforts

Cybersecurity information sharing, as a general concept, was introduced above. This paper presents a suite of metrics for use by (DHS-led) critical-infrastructure-centric cybersecurity information sharing efforts. What do such efforts look like, in a more specific sense? To illustrate, and to set the stage for later discussion, consider the DHS-led, public-private CIKR Cyber Information Sharing and Collaboration Program (CISCP).[10] The CISCP—and efforts like it—seek to "promote the safety, security, and resiliency of the Nation's critical infrastructure by establishing a robust operational cyber information sharing program that measurably improves situational awareness and incident response coordination capabilities among government and CIKR owners and operators to reduce risks posed by cyber threats" (DHS 2011c).[11]

Entities participating in critical-infrastructure-centric cybersecurity information sharing efforts include for-profit and not-for-profit organizations from industry and academia—such as individual critical infrastructure owner/operators, information sharing and analysis organizations (some formal ISACs, some not formally categorized as ISACs but similar in concept), security application vendors, managed security service providers (MSSPs), and internet service providers (ISPs)—as well as DHS (through which data from other U.S. government departments and agencies flow).

Interestingly, and perhaps unique to cybersecurity, the cyber-related protection of critical infrastructure may best be accomplished not by critical infrastructure owner/operators themselves, but rather by other vendors or service providers. Analysis of the pool of participants in specific information sharing efforts and the extent to which broader critical infrastructure assets are somehow directly or indirectly protected through them is outside the scope of the present paper and remains an important topic for future research.

Participation in critical infrastructure cybersecurity information sharing efforts is frequently governed under formal legal frameworks, such as cooperative research and development agreements (CRADAs).[12] For example, the aforementioned CISCP employs a CRADA through which participants gain access to a CISCP compartment on the US-CERT website—the primary vehicle for CISCP information sharing—and also are given the option to place an analyst on the National Cybersecurity and Communications Integration Center (NCCIC) floor.[13] By signing the CRADA, participants are expected to "engage in cybersecurity data flow, analytical collaboration, and incident management activities" (DHS 2011g).

---

[10] This research was conducted for the DHS/CS&C/Critical Infrastructure Cyber Protection & Awareness branch, under whose purview is the CISCP. The CISCP is a representative example of critical-infrastructure-centric cybersecurity information sharing efforts.

[11] This appears to be restated by DHS (2011d) as the following "operational goals": "create shared situational awareness across CIKR sectors; enhance collaboration among the US Government and CIKR owners and operators; and leverage private/public sector expertise to collaboratively respond to incidents."

[12] CRADAs are "agreements between one or more Federal laboratories [or agencies] and one or more non-Federal parties under which the Government…provides personnel, services, facilities, equipment, intellectual property, or other resources with or without reimbursement…and the non-Federal parties provide funds, personnel, services, facilities, equipment, intellectual property, or other resources toward the conduct of specified research or development efforts which are consistent with the mission [of the agency]" (15 U.S.C. §3710).

[13] US-CERT is the United States Computer Emergency Readiness team, which is operated by DHS. The NCCIC is a DHS-led cyber watch-and-warning center. For an overview of the NCCIC, see "Secretary Napolitano Opens New

Specific critical infrastructure cybersecurity information sharing efforts reside in a larger universe, of course, in which numerous other public-private or private-private information sharing efforts exist—some of which overlap.[14] Overlapping efforts may affect the efficacy of information sharing and the cybersecurity of entities participating in various efforts (this point is also made, in reference to both information sharing efforts and coordinating bodies, such as the NIAC, in the *Cyberspace Policy Review*).[15] Study of the existence of multiple overlapping information sharing efforts and their impact on each other is outside the scope of this paper, as is study of strategic relationship management from a process perspective. These remain important topics for future research.

In terms of information flows, critical-infrastructure-centric cybersecurity information sharing typically occurs via: 1) access to a compartment on the US-CERT or similar website (or perhaps via e-mail or chat sessions); 2) periodic collaborative exchanges; and 3) in-person collaboration between participants on the NCCIC or similar watch floor. These are discussed in turn.

Regarding sharing via the US-CERT website—the core of many DHS-led critical infrastructure cybersecurity information sharing efforts—information flows from participants to DHS and from DHS to participants, all through exchange with a specific compartment on the US-CERT website (see figure 1). By and large, information sent by participants to DHS includes "repeatable, deterministic indicators of compromises or attempted compromises; domains and IPs with the 'last resolved' timestamps; domains with 'fast flux yes or no' answers; MD5 hashes with byte lengths and sizes; [and] narrative context wherever necessary to support the above" (DHS 2011c). Information sent by DHS to participants comprises analytic products—ranging from more tactical priority alerts, indicator bulletins, and analysis

---

National Cybersecurity and Communications Integration Center," DHS Office of the Press Secretary, 30 October 2009, http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm.

[14] Critical-infrastructure-centric cybersecurity information sharing takes place through various private-private, public-private, and public-public fora. A representative list involving DHS and others includes: (various portals of the website of the) U.S. Computer Emergency Readiness Team (US-CERT); Integrated Control Systems Cyber Emergency Response Team (ICS-CERT); DHS Joint Cybersecurity Services Pilot (JCSP); DHS CIKR Cyber Information Sharing and Collaboration Program (CISCP); Department of Defense (DoD)-Defense Industrial Base Collaborative Information Sharing Environment (DCISE); Defense Secure Information Exchange (DSIE); Network Security Information Exchange (NSIE); information sharing and analysis centers (ISACs); fusion centers; and Infragard. Other efforts are being discussed on Capitol Hill; see, for example, U.S. House of Representatives Republican Cybersecurity Task Force (2011), H.R. 3523 (the Cyber Intelligence Sharing and Protection Act of 2011), S. 2105 (the Cybersecurity Act of 2012), and S. 2150 (the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012).

[15] The importance of reconciling multiple information sharing efforts is highlighted in the *Cyberspace Policy Review* (White House 2009): "These [multiple information sharing] groups perform valuable work, but the diffusion of effort has left some participants frustrated with unclear delineation of roles and responsibilities, uneven capabilities across various groups, and a proliferation of plans and recommendations. As a result, government and private-sector personnel, time, and resources are spread across a host of bodies engaged in sometimes duplicative or inconsistent efforts. Partnerships must evolve to clearly define the nature of the relationship, the roles and responsibilities of various groups and their participants, the expectations of each party's contribution, and accountability mechanisms. The Federal government should streamline, align, and provide resources to existing organizations to optimize their capacity to identify priorities, enable more efficient execution, and develop response and recovery plans."

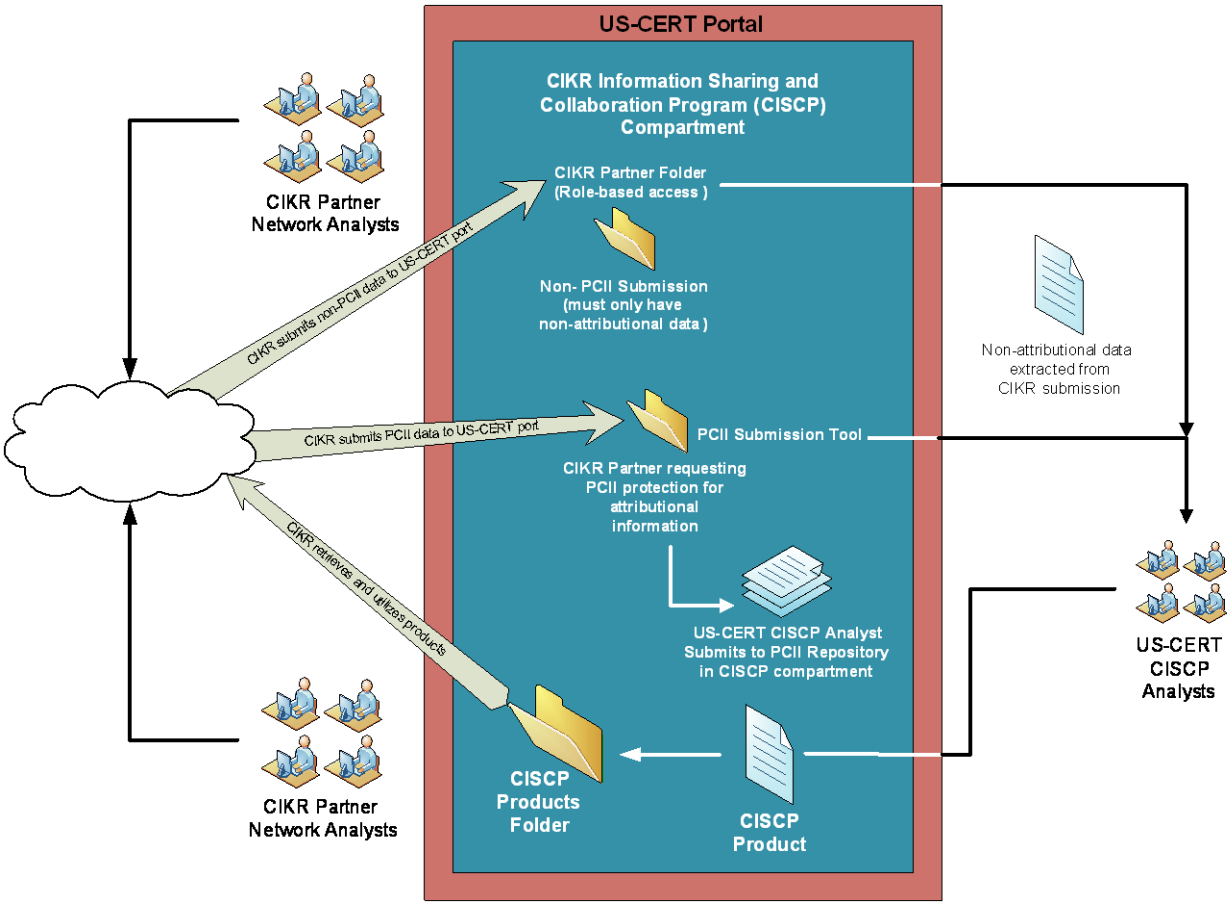
bulletins to more strategic recommended practices (see table 1)—produced by DHS analysts. These products are largely based on participant-provided information, though "anonymized" to minimize risks to participants; they are not formally "sent" to participants, but rather posted in a products folder on the website. Additionally, requests for information (RFIs) are sent by DHS to participants (to capture feedback on analytic products) and by participants to DHS (to ask ad hoc questions of DHS and other participants). RFIs assess the extent to which disseminated information adds value, among other things.

Regarding collaboration—periodic collaborative exchanges and in-person collaboration on the NCCIC floor—information flows are less structured and more multilateral. The subject matter of collaboration generally mirrors that of web-based information sharing—threats, vulnerabilities, incident response, and best practices—though it is perhaps less tactically focused. Collaboration may influence analytic products; it also works to generate trust and foster deeper working relationships, including through the provision of expert input and reach-back support on issues raised on the NCCIC floor.

Importantly, most critical infrastructure information sharing efforts are voluntary, and participants share only what, and with whom, they choose to share. This is true of sharing via the US-CERT website as well as collaboration in more ad hoc settings, such as on the NCCIC floor. The choice to filter information is driven by a number of factors, including real or perceived legal barriers, reputational risks, and so on. Further, it may be the case that the quality of information shared is lacking, perhaps because the cybersecurity capabilities of participants are maturing.[16] The efficacy of information sharing efforts is in part a function of participants' willingness to share and the quality of the information shared (this is discussed in greater detail later in the present paper; see page 26, as well as footnotes 39 and 46).

[16] Along these lines, the maturity of participants' cybersecurity capabilities may also affect the amount of information shared: a participant may wish to share all relevant cyber incident information with others, but may not even be aware that incidents are occurring on its systems.

Figure 1. An Example of Critical-Infrastructure-Centric Cybersecurity Information Flows (from the CISCP)



Source: DHS 2011c. PCII refers to "protected critical infrastructure" information.

Table 1. An Example of DHS-Generated Analytic Products (from the CISCP)

CISCP analytic product	***Intent***
Priority Alert	Alert-type product focused on providing early warning of a single specific threat or vulnerability expected to have significant CIKR impact
Indicator Bulletin	Short and timely information product regarding indicators of new threats and vulnerabilities based on reporting from government and CIKR
Analysis Bulletin	More in-depth analytic product that ties together related threat and intruder activity, describing the activity, how to detect it, defensive measures, and remediation advice
Recommended Practices	[A products that is] intended to provide a method for collaboratively defining and documenting a series of "best practice" recommendations/strategies for threat/vulnerability risk management and response/recovery

Source: DHS 2011c.

D. Research Questions, Methodology, and Scope

As noted, DHS facilitates various critical-infrastructure-centric cybersecurity information sharing efforts. To help gauge their efficacy, and to facilitate their management, CS&C asked HSSAI to develop a suite of metrics. Specifically, this research sought to answer the following question:

- What holistic, theory-driven suite of performance measurement metrics should be used to gauge the efficacy of (DHS-led) critical-infrastructure-centric cybersecurity information sharing efforts?

To develop the metrics, HSSAI:

- **Reviewed extant literature on and interviewed entities involved in information sharing efforts**: HSSAI reviewed the existing academic, industry, and policy-relevant literature on metrics in general and on the use of metrics in analogous cyber and non-cyber information sharing environments. HSSAI also explored the broad multidisciplinary literature on information, information theory, the value of information, decision theory, and uncertainty. The literature review was complemented by interviews with individuals in analogous environments.

- **Examined mission activities**: HSSAI sought to understand mission, vision, goals, objectives, roles, responsibilities, and stakeholders of critical-infrastructure-centric cybersecurity information sharing efforts. This subtask helped identify the attributes of mission success and failure—and what broad parameters could be measured to indicate such outcomes.

- **Examined information and information flows**: HSSAI examined the specific kinds of information that are shared and the mechanisms and procedures for sharing information among entities participating in critical-infrastructure-centric cybersecurity information sharing efforts. This subtask suggested how metadata/descriptive statistics relating to signatures, etc. could serve as or somehow contribute to metrics.

- **Assembled a suite of metrics for use in evaluating the information sharing and related activities**: Based on the input gleaned from the array of subtasks above, HSSAI generated a holistic, theory-driven suite of metrics to support information sharing performance measurement.

In terms of scope:

- This research focuses on metrics for gauging the efficacy of a cybersecurity information sharing effort. The research does not represent a treatise on cybersecurity metrics writ large.

- To allow for broadest possible use, it was determined that the metrics and their data sources would all be unclassified (though the metrics recommended here could be used to gauge the efficacy of information sharing in classified settings as well).

The research was carried out on a part-time basis between May 2011 and February 2012.

III. Theoretical Underpinnings

This chapter seeks to set the stage, in some depth, for the development of methodologically sound metrics for critical-infrastructure-centric cybersecurity information sharing. It begins by discussing performance measurement and metrics, including best practices in their development and use. It then considers the general concept of information sharing—including reasons that information should be shared and potential downsides of such sharing—drawing from the literature on information, information theory, the value of information, decision theory, and uncertainty. HSSAI was asked to provide DHS with a theory-driven suite of metrics; this chapter is the detailed foundation upon which the suite of metrics is built.

A. Performance Measurement and Metrics

The present paper sets forth a suite of metrics for measuring the efficacy of DHS-led cybersecurity information sharing efforts. This is the province of *performance measurement*. Performance measurement is defined as "regular measurement of the results (outcomes) and efficiency of services or programs" (Hatry 2006). Performance measurement is the central plank of *performance management*, itself defined as "the use of performance information to affect programs, policies, or any other organization actions aimed at maximizing the benefits of public services" (Hatry 2003).

Performance is measured for various reasons, including to evaluate, control, budget, motivate, promote, celebrate, learn, and improve (Behn 2003).[17] Chief among these is *improve*, "the core purpose behind the other seven" (Behn 2003). That is, performance is measured so performance can be actively managed to drive increases—improvements—in taxpayer or shareholder value. After all, performance measurement is a means to an end, not the end in itself.[18] Along these lines, performance measurement must occur repeatedly over time.

Performance measurement techniques are widely employed in the public and private sectors.[19] In certain circumstances, performance measurement is required. For example, the Government

[17] Behn (2003) further elaborates on these eight reasons for performance measurement with notional explanatory queries for each as follows: evaluate ("how well is my public agency performing?"); control ("how can I ensure that my subordinates are doing the right thing?"); budget ("on what programs, people, or projects should my agency spend the public's money?"); motivate ("how can I motivate line staff, middle managers, nonprofit and for-profit collaborators, stakeholders, and citizens to do the things necessary to improve performance?"); promote ("how can I convince political superiors, legislators, stakeholders, journalists, and citizens that my agency is doing a good job?"); celebrate ("what accomplishments are worthy of the important organizational ritual of celebrating success?"); learn ("why is what working or not working?"); and improve ("what exactly should who do differently to improve performance?").

[18] Notes Hatry (2006): "If measurement information is not used, the effort and cost of the performance measurement process will be wasted. Use of performance information—whether by program managers, agency officials, officials in central government, elected officials, members of boards or citizens—transforms performance measurement into performance management." Similar sentiments pervade the literature. Behn (2003), for example, suggests that "neither the act of measuring performance nor the resulting data accomplishes anything itself; only when someone uses these measures in some way do they accomplish something."

[19] For information on performance measurement in government/nonprofit entities, see, for example, Hatry (2006, 2003, 1980), Behn (2003), Moore (2003), and Kaplan (2009). For information on performance measurement in the private sector, see Kaplan and Norton (1992) and Kaplan (2010). See also Robert Behn, "Bob Behn's Performance Leadership Report," www.hks.harvard.edu/thebehnreport/; Urban Institute, "Performance Measurement–

Performance and Results Act of 1993 (GPRA, modified via the Government Performance and Results Modernization Act of 2010) sets forth certain requirements for federal government departments and agencies to develop strategic plans, performance plans, and program performance reports with supporting performance indicators.[20] As the Government Accountability Office (GAO) notes, "[GPRA] shifts the focus of government decision-making and accountability away from a preoccupation with the activities that are undertaken—such as grants dispensed or inspections made—to a focus on the results of those activities, such as real gains in employability, safety, responsiveness, or program quality" (GAO 2001). In cybersecurity, the Federal Information Security Management Act of 2002 (FISMA) requires reporting, to the Office of Management and Budget (OMB), of cyber-related performance measures by federal departments and agencies.

Performance measurement employs specific *metrics*—the indicators, the data points, the *sine qua non*—to quantitatively or qualitatively measure performance-related parameters of interest.[21] These parameters of interest—and the metrics that measure them—are commonly grouped into four different categories as follows (Hatry 2006):

- **Inputs** represent resources invested into the program or activity being measured, such as funds, employee-hours, or raw materials.
- **Outputs** represent the completed or delivered products or services generated through inputs.
- **Processes** (sometimes referred to as activities) represent the steps that turn inputs into outputs.
- **Outcomes** (sometimes disaggregated into **intermediate** and **end** outcomes, the latter of which are sometimes referred to as **impacts**) represent the "events, occurrences or changes in condition" that indicate programmatic progress, brought about at least in part through outputs.[22]

Performance Management," www.urban.org/government/measurement.cfm; White House Office of Management and Budget, "Performance & Personnel Management," www.whitehouse.gov/omb/performance; and Balanced Scorecard Institute, "Home," www.balancedscorecard.org. For information on performance measurement in cybersecurity and information security, see Information Assurance Technology Analysis Center (DoD 2009) and NIST (2008a). For more on performance *management*, see, for example, Forsythe (2001) and its extensive references.

[20] As stated in the act itself, GPRA was developed explicitly to "(1) improve the confidence of the American people in the capability of the Federal Government, by systematically holding Federal agencies accountable for achieving program results; (2) initiate program performance reform with a series of pilot projects in setting program goals, measuring program performance against those goals, and reporting publicly on their progress; (3) improve Federal program effectiveness and public accountability by promoting a new focus on results, service quality, and customer satisfaction; (4) help Federal managers improve service delivery, by requiring that they plan for meeting program objectives and by providing them with information about program results and service quality; (5) improve congressional decisionmaking by providing more objective information on achieving statutory objectives, and on the relative effectiveness and efficiency of Federal programs and spending; and (6) improve internal management of the Federal Government."

[21] Sources in the literature occasionally differentiate between "measures" and "metrics"; this paper does not.

[22] Similar definitions exist in sources throughout the literature, including the policy literature (e.g., OMB Circular No. A-11, Part 6 [OMB 2011]). Also, outputs do not always lead to desired outcomes, and outcomes are not always caused by outputs. For example, in a private-sector entity, increased product quality and improved customer

Input/process/output/outcome metrics can be used in various ways to convey—to measure—a number of overlapping concepts, including, but by no means limited to: effectiveness, efficiency, quality, timeliness, productivity, costs, workload, and the like. Metrics can measure one-dimensional concepts, such as number of hours worked, or multidimensional concepts, such as number of units produced per hour worked (Department of Energy 1996). In this regard, metrics from one time period can be compared to metrics in a previous time period, to some agreed standard or target, or to metrics from other similar programs. Such approaches are used to suggest whether performance is satisfactory, and allow for course corrections as necessary.[23]

Perhaps not surprisingly, specific metrics must be carefully selected. This is because:

- **Different metrics serve different purposes**. As noted, performance is measured for reasons including evaluate, control, and budget; each reason may command the use of different metrics (Behn 2003).

- **The easiest concepts to measure are not always the concepts of interest**. Specific metrics must be chosen with the goals and objectives of an organization in mind, as well as the purpose for performance measurement. They should not be chosen simply because they are easy, and thus inexpensive, to measure—though cost is relevant (see below).

- **Metrics require data, and data collection requires effort**. Put another way, data collection for performance measurement (or any other activity) is not cost-free. Metrics must be selected in a way that is mindful that performance measurement should not cost more than the benefits it is intended to bring about.

- **What gets measured gets done, and what does not get measured typically does not get done**. Good performance is often rewarded (or bad performance punished), and thus individuals focus efforts on those things that are being measured, sometimes at the expense of everything else (though unmeasured things are not all ignored). Metrics must be selected such that they don't have counterproductive results.

---

satisfaction are outputs that could certainly lead to improved sales. However, the improved sales could be also attributable to the recent bankruptcy of a major competitor. For more on causality, see footnote 23.

[23] Performance measurement methods, though very useful, do not formally—statistically—isolate the impact of a program. More methodologically sound approaches to isolating program impact may be found in the field of impact analysis (also known as program evaluation). Impact analysis represents the act of "determining the extent to which one set of directed human activities (X) affected the state of some objects or phenomena ($Y_1 \ldots Y_k$) and—at least sometimes—determining also why the effects were as small or large as they turned out to be" (Mohr 1995). Impact analysis provides more concrete thinking on—and quantitative statistical approaches to—isolating the marginal impact of a program itself. This involves understanding the concept of the counterfactual (i.e., what would have happened in the absence of the program), as well as tenets of experimental design (i.e., approaches—such as the use of control groups, random assignment, and pre-/post-program tests—that allow for isolating causality and marginal impacts of the program itself, given the wider world in which the program exists). The present paper draws on impact analysis concepts and tenets as appropriate. For more on program evaluation/impact analysis, see Cook and Campbell (1979), Campbell and Stanley (1966), Rossi and Freeman (1993, 2004), and Mohr (1995).

Accordingly, metrics should exhibit particular properties. In sum, metrics should be "fit for purpose" (i.e., fit for the purpose of performance measurement). Fitness for purpose relates to the field of data quality (where data quality is synonymous with fitness for purpose). Data quality is commonly discussed and evaluated along six dimensions: relevance, accuracy, timeliness, accessibility, comparability, and coherence (see table 2, below).[24] After all, metrics yield performance data; those data should be relevant, accurate, timely, accessible, comparable, and coherent for measuring performance.[25] Metrics focused on examining the performance of an information sharing effort may measure the quality of the actual information being shared, like the timeliness of that information, or its relevance.

Importantly, metrics are not typically used in isolation, but rather in a suite. This is because single measures of performance generally fail to convey sufficient meaningful performance information to managers (Kaplan and Norton 1992).[26] In essence, if good performance in an organization or a program is a function of a vector of specific parameters that cause such good performance, then a suite of metrics used to measure performance should relate to those specific parameters. Further, a suite of metrics should be comprehensive but not overwhelming (Behn 2007a); it should contain certain priority measures complemented by a number of broader indicators (Behn 2007b).

Lastly, a suite of metrics is often developed using a graphical representation of the hypothesized causal chain leading from inputs (on the left) to outcomes (on the right) known as an *outcome line* (see figure 2). Once fully specified, an outcome line helps to clarify: 1) what is expected to result from X (inputs and processes); and 2) how Y (the outcome of interest) can be expected to follow from X (Mohr 1995). Use of an outcome line seeks to ensure that the specific metrics selected in performance measurement efforts capture appropriate—i.e., causally related (hypothetically)—inputs, processes, outputs, and outcomes. Of note is whether any box, when fully specified, can be fully—and causally—supported by one to its immediate left in the outcome flow. If this is the case, then only the box on the immediate left must be measured.

[24] For more on the study of data quality, see, for example, Wang and Strong (1996), Wand and Wang (1996), Otto et al. (2009), and the information quality website hosted by the Massachusetts Institute of Technology: http://mitiq.mit.edu/. For an international perspective, see references listed on the "Data Quality Reference Site" of the International Monetary Fund: http://dsbb.imf.org/Pages/DQRS/home.aspx. Certain data quality evaluation schemes employ five dimensions, others seven or even more—but all are similar.

[25] Along these lines, Hatry (1980) presents the following criteria for selecting performance measures: validity/accuracy, understandability, timeliness, potential for encouraging perverse behavior, uniqueness, data collection costs, controllability, comprehensiveness. Not uncommon in the business world is use of the acronym SMART to connote that metrics should be specific, measureable, achievable, realistic, and timely.

[26] This is thought to be the case even in for-profit businesses, in which semi-meaningful single measures of performance (like profit) exist. The belief that multiple measures are necessary for sound performance measurement is the foundation of Kaplan and Norton's seminal "balanced scorecard" (see, for example, Kaplan and Norton 1992; Kaplan 2010).

Table 2. Six Dimensions of Data Quality

Dimension and definition	*Key components*
1. Relevance The degree to which the statistical product meets user needs for both coverage and content.	Any assessment of relevance needs to consider: ▪ who are the users of the statistics ▪ what are their needs ▪ how well does the output meet these needs
2. Accuracy The closeness between an estimated result and the (unknown) true value.	Accuracy can be split into sampling error and non-sampling error, where non-sampling error includes: ▪ coverage error ▪ non-response error ▪ measurement error ▪ processing error ▪ model assumption error
3. Timeliness and punctuality Timeliness refers to the lapse of time between publication and the period to which the data refer. Punctuality refers to the time lag between the actual and planned dates of publication.	An assessment of timeliness and punctuality should consider the following: ▪ production time ▪ frequency of release ▪ punctuality of release
4. Accessibility and clarity Accessibility is the ease with which users are able to access the data. It also relates to the format(s) in which the data are available and the availability of supporting information. Clarity refers to the quality and sufficiency of the metadata, illustrations and accompanying advice.	Specific areas where accessibility and clarity may be addressed include: ▪ needs of analysts ▪ assistance to locate information ▪ clarity ▪ dissemination
5. Comparability The degree to which data can be compared over time and domain.	Comparability should be addressed in terms of comparability over: ▪ time ▪ spatial domains (e.g. sub-national, national, international) ▪ domain or sub-population (e.g. industrial sector, household type)
6. Coherence The degree to which data that are derived from different sources or methods, but which refer to the same phenomenon, are similar.	Coherence should be addressed in terms of coherence between: ▪ data produced at different frequencies ▪ other statistics in the same socio-economic domain ▪ sources and outputs

Source: From Fleming (2009), citing UK Office of National Statistics (2005).

Figure 2. A Notional Outcome Line

Source: Adapted from Mohr (1995). Use of an outcome line seeks to ensure that the specific metrics selected in performance measurement efforts capture appropriate—causally related (hypothetically)—inputs, processes, outputs, and outcomes. If any box, when fully specified, can be fully (causally) supported by one to its immediate left in the flow, then only the box on the immediate left must be measured.

B. Information Sharing

This paper presents metrics relating to information sharing efforts. Information sharing as a general security concept has received considerable attention in recent years. This is the case not least because information sharing shortcomings are thought to have contributed to the failure to prevent the events of 11 September 2001.[27] Symbolized by a move from a "need-to-know" to a "need-to-share" paradigm, as well as explicit recognition of the importance of public-private information sharing partnerships, a variety of efforts and initiatives in the decade since 9/11 have sought to address these shortcomings. These include the establishment of a Program Manager-Information Sharing Environment (PM-ISE) within the Office of the Director of National Intelligence (ODNI) and the creation of fusion centers in states and major urban areas nationwide, among many other things.

The literature—comprised primarily of policy documents—notes that information sharing facilitates the provision of security. For example, the 2010 *National Security Strategy* states that "our country's safety and prosperity depend on the quality of the intelligence we collect and the analysis we produce, our ability to evaluate and share this information in a timely manner, and our ability to counter intelligence threats. This is as true for the strategic intelligence that informs executive decisions as it is for intelligence support to homeland security, state, local, and tribal governments, our troops, and critical national missions" (White House 2010). The 2010 *Quadrennial Homeland Security Review* (QHSR) identifies information sharing as driver for security risk management, reporting that "the engine behind a distributed homeland security effort is a shared awareness of the risks and threats among all key stakeholders" (DHS 2010c).[28] The 2009 *NIPP* notes that "the effective implementation of the NIPP is

[27] See the final report of the 9/11 Commission for more discussion of the impact of information sharing weaknesses on the attacks of 11 September 2001 (9/11 Commission 2004).

[28] Similar sentiments pervade the literature; see, for example, the *National Intelligence Strategy* (ODNI 2009); *National Strategy for Homeland Security* (White House 2007a); *National Defense Strategy* (DoD 2008); *Quadrennial Defense Review* (DoD 2010); *National Strategy for Information Sharing* (White House 2007b); the information sharing strategies of the intelligence community (ODNI 2008), DoD (DoD 2007), DHS (DHS 2008), and Federal Bureau of Investigation (FBI; FBI 2011a); the *Annual Report to Congress* of PM-ISE (PM-ISE 20110); the Nationwide SAR Initiative *Annual Report* (Department of Justice 2010); the PM-ISE *Implementation Plan* (PM-ISE 2006), the *NIPP* (DHS 2009a); and the IT-sector *Sector Specific Plan* (DHS 2010b). Additional sources of relevance include various information sharing GAO (e.g., GAO 2008 and 2006) and the Markle Foundation's work on information sharing (Markle Foundation 2003 and 2002).

predicated on active participation by government and private-sector partners in meaningful, multidirectional information sharing" (DHS 2009a).

With specific regard to cybersecurity, virtually every significant national review or report in recent years has highlighted the importance of information sharing to securing cyberspace. Along these lines, the White House *Cyberspace Policy Review* notes that "information is key to preventing, detecting, and responding to cyber incidents. Network hardware and software providers, network operators, data owners, security service providers, and in some cases, law enforcement or intelligence organizations may each have information that can contribute to the detection and understanding of sophisticated intrusions or attacks. A full understanding and effective response may only be possible by bringing information from those various sources together for the benefit of all" (White House 2009).[29]

But while the intrinsic importance of information sharing has been widely recognized, few sources define information sharing—as a concept—with any specificity.[30] Such specificity facilitates the identification of inputs/processes/outputs/outcomes that can be measured. For the purposes of the present paper, ***information sharing*** **represents the process through which information is provided by one entity to one or more other entities to facilitate decision making under conditions of uncertainty**, where:

- ***Information*** **represents "data + meaning"** (Floridi 2009).[31] For example, in the context of cybersecurity information sharing, an IP address would be data; the fact that it is a suspected hostile IP address (which users should be prevented from visiting) would be associated meaning.

[29] For additional such cybersecurity-specific information sharing thoughts, see also the report and two-year follow-up of the *Commission on Cybersecurity for the 44th Presidency* of the Center for Strategic and International Studies (CSIS; CSIS 2008 and 2011); the Comprehensive National Cyber Initiative (as described in the unclassified summary of HSPD 23/NSPD54; White House 2007); the DHS *Blueprint for a Secure Cyber Future* (DHS 2011a); and *Enabling Distributed Security in Cyberspace* (DHS 2011h). Certain members of Congress also concur; see House Republican Cybersecurity Task Force (2011), H.R. 3523 (the *Cyber Intelligence Sharing and Protection Act of 2011*), and S. 2105 (the *Cybersecurity Act of 2012*), which call for strong cybersecurity information sharing.

[30] This is not to suggest that *no* definitions may be found in the literature. The 2010 PM-ISE *Annual Report to Congress*, for example, states that "the term 'information sharing' in the context of the ISE means that the necessary information, properly controlled, gets to the right people in time to counter terrorist threats to our people and institutions" (PM-ISE 2011). The 2007 DoD *Information Sharing Strategy* defines information sharing as "making information available to participants (people, process, or systems)…[it] includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant" (DoD 2007a). The 2008 Intelligence Community *Information Sharing Strategy* states that "information sharing is a behavior and not a technology. In the Intelligence Community, information sharing behavior is the act of exchanging intelligence information between collectors, analysts, and end users in order to improve national and homeland security" (ODNI 2008).

[31] In truth, multiple definitions of "information" prevail in the literature, a point made by Claude Shannon (1993, as cited in Floridi 2009), among others: "The word 'information' has been given different meanings by various writers in the general field of information theory. It is likely that at least a number of these will prove sufficiently useful in certain applications to deserve further study and permanent recognition. It is hardly to be expected that a single concept of information would satisfactorily account for the numerous possible applications of this general field." Information as "data + meaning" can be considered a "general definition of information" (Floridi 2009). For more on information and information theory, see Shannon (1948), Weiner (1950), Floridi (2009, 2010, and 2011).

- ***Decision making*** **represents goal-directed behavior in the presence of options** (adapted from Hansson 2005); it involves choosing between an array of competing actions (including taking no action).[32] From the example above, decision making would involve choosing to prevent—or not—users from visiting the suspected hostile IP address.

- ***Uncertainty*** **represents the state of being not known, indeterminate, questionable, variable**; adapted from Merriam-Webster 2002); it results from incomplete information, measurement error, linguistic imprecision, variability, randomness. (Granger-Morgan and Henrion 1992).[33] From the example above, uncertainty would relate to the fact that the suspected hostile IP address could, in fact, be innocuous (blocking it would deny user intent, perhaps affecting user productivity), or it could be hostile—and there is a cost to taking action (i.e., to the decision).[34]

This specific definition of information sharing carries with it certain important—and sometimes overlapping—implications for the selection of metrics for information sharing performance measurement. These include the following (summarized in table 3, below; specific metrics are presented later in the present paper, guided by these implications):

- **Information sharing should be goal-directed**.[35] That is, information sharing is not an end in itself, but a means to an end; this end is the goal described in the goal-directed behavior of decision making.[36] Thus, entities in an information sharing effort should recognize, understand, and concur with a common goal (though entities may have other goals; goals don't need to be uniform across entities, as long as they do not contravene each other). Further, and critically, in thinking of performance measurement, the goal represents the outcome; it is used to specify outcome metrics. In a security setting, achieving the goal implies continuous activity, not a simple one-off voyage from a starting point to a destination.

---

[32] For more on decision theory, see Hansson (2005) and the body of literature cited therein.

[33] From Granger-Morgan and Henrion (1992): "'Uncertainty' is a capricious term, used to encompass a multiplicity of concepts. Uncertainty may arise because of incomplete information—what will be the U.S. defense budget in the year 2050?—or because of disagreement between information sources—what was the 1987 Soviet defense budget? Uncertainty may arise from linguistic imprecision—what exactly is meant by 'The river is wide'? It may refer to variability—what is the flow rate of the Ohio River? Uncertainty may be about a quantity—the slope of a linear dose-response function—or about the structure of a model—the shape of a dose-response function. Even where we have complete information in principle, we may be uncertain because of simplifications and approximations introduced to make analyzing the information cognitively or computationally more tractable. As well as being uncertain about what is the case in the external world, we may be uncertain about what we like, that is about our preferences, and uncertain about what to do about it, that is, about our decision. Very possibly, we may even be uncertain about our degree of uncertainty."

[34] False positives (type I errors) and false negatives (type II errors) both exact a cost, of course.

[35] The word "goal" is used broadly to represent concepts such as goals, objectives, and missions.

[36] The *NIPP* (DHS 2009a) espouses a similar view: "Within the CIKR community, information sharing is a means to an end. The objective of an effective environment for information sharing is to provide timely and relevant information that partners can use to make decisions and take the necessary actions to manage CIKR risk."

- **Information should be shared with entities who can effect achievement of the goal or affect how the goal is achieved—but not with those who cannot**. An information sharing effort should comprise appropriate entities, namely those who somehow possess sufficient relevance, authority, responsibility, and capability to act in achievement of the goal (i.e., entities with a mission need).[37] Such appropriate entities should, in fact, participate in the information sharing effort, whether through machine-to-machine dissemination of information or longer-term human-to-human collaborative problem solving and response to requests for information. (Indeed, a complete lack of participation calls into question the purpose of an information sharing effort in the first place.) But information should not be shared outside of appropriate entities, purposely (through insider or external threats) or accidentally. Doing so represents the "loss of control" of information.[38] Loss of control incurs certain costs, including intelligence loss to adversaries, reputational damage to sharing entities, violations of privacy/civil liberties/civil rights, which should be minimized.[39]

- **Relatedly, shared information should be used for purposes that can effect or affect achievement of the goal—but not for purposes that cannot**. Use should generally be both tactical and strategic, as achievement of a goal typically commands the use of both tactics and strategy. In a security setting, information sharing should seek to minimize specific threats, vulnerabilities, and consequences (tactical uses)—as well as highlight broader trends among them, not least to guide resource-allocation decisions (strategic uses).[40] Of course, shared information should only be used for appropriate purposes—there should be no loss of control.

- **Shared information should be fit for the purpose of reducing uncertainty**. Specifically, information must comprise both "data" and "meaning," as one without the other is of little use.[41] Moreover, information must be of sufficient quality; it should be relevant, timely, accessible, and accurate.[42]

---

[37] A similar thought is put forward by Markle (2002): "Therefore, the network structure must be augmented by arrangements that ensure the following: 1.) that information in fact flows to all who need it; and 2.) that information is provided to decisionmakers and policymakers with responsibility and authority to act, who are ultimately accountable to the public for the performance of the system." Also, note that appropriate entities may include those who can effect or affect change more indirectly, in a nonobvious way.

[38] The concept of loss of control—which relates to the confidentiality and potential integrity of information—concerns both users and uses of information. That is, loss of control may be a function of sharing with inappropriate entities (i.e., unauthorized users) and sharing for inappropriate purposes (i.e., unauthorized uses).

[39] In a security setting, shared information often relates to incidents (i.e., in some way relates to threats, vulnerabilities, and consequences); loss of control of this type of information may lead to reputational harm on the part of appropriate entities. Reputational harm may undermine trust among appropriate entities in an information sharing effort, which may undermine the extent to which they share information (which in turn may undermine efforts to achieve the goal of the information sharing in the first place).

[40] See also the *NIPP* (DHS 2009a): "The CIKR Information-Sharing Environment (ISE) supports three levels of decisionmaking and action: (1) strategic planning and investment, (2) situational awareness and preparedness, and (3) operational planning and response."

[41] This is not to suggest that meaning must be exhaustive, just that a lack of meaning is suboptimal.

[42] "Quality" here refers to "data quality" (this is discussed earlier in the present paper; see page 15). To avoid confusion—despite broad use of the term "data quality" in the field—this section refers more generally to "information quality" (not "data quality"), though with the same implications. Note that the information quality

For example, relevance implies that shared information should meet user needs—guided by the goal to be achieved—for coverage and content (among other things, it should represent new information: new data, new meaning, or both). Accuracy implies that shared information should be as close as possible to the (unknown) true value (it should represent neither false positive nor false negative). Accessibility implies that shared information should be available and easily usable (it should be formatted for convenient and immediate use). And timely implies that shared information should be current (released as close as possible to the period to which the information refers, with only limited time between an incident and the sharing of information about that incident).[43]

- **Information sharing cannot reduce all uncertainty, and, in some cases, it may increase it**. This is the case for a variety of reasons. To begin, some uncertainty cannot be reduced, even with perfect/full information sharing. For example, in cybersecurity, a "zero-day" exploit implies a new and novel exploit that has never been seen before. By definition, no information exists—and thus none can be shared—on zero-day exploits until they are exploited (and are noticed), and knowledge of their existence prior to their initial discovery is *prima facie* impossible (see also Rosenzweig [2011] and Bayuk's [2011] discussion of *Zero Day Threat* by Acohido and Swartz).[44] Further, the sharing of inaccurate information (false positives or false negatives) does not, in general, reduce uncertainty, not least because one cause of uncertainty itself is error in measurement.[45] Also, information sharing can, in certain circumstances, lead to information overload. Information sharing typically requires personnel to manage, analyze, and leverage information; overload may imply that personnel are overwhelmed and unable to use information to affect or effect achievement of the goal. Along these lines, though of potentially lesser importance as processor speeds and storage

---

dimensions of comparability and coherence are deemed here to be of lesser relevance to measuring the performance of information sharing efforts. Also, put another way, information should "add value." A small body of literature discusses this concept—the value of information—which itself overlaps with the study of information/data quality. The literature is summarized by Macauley (2005), who notes: "Information is without value: when individual's subjective beliefs are at extremes (p = 0 or p = 1); when there are no costs associated with making the wrong decision; when there are no actions that can be taken in light of the information. Information has less value: when individual's subjective beliefs are close to extremes; when the costs of making the wrong decision are low; when actions to take are very limited. Information has the most value: the more indifferent is the decisionmaker among her alternatives (flips a coin); the larger are the costs of making the wrong decision; the more responsive are the actions that can be taken."

[43] Information sharing efforts often seek to disseminate "actionable" information; in essence, actionable is comprised of the (more measurable) components of data + meaning, relevance, timeliness, accessibility, and accuracy.

[44] More prosaically, think also of the roll of a fair die. Information sharing between entities with experience rolling a die can suggest that the outcome will be evenly distributed among integer values between one and six—but no amount of information sharing can suggest what the exact outcome of the next roll will be, as it is random. This type of uncertainty is often called aleatoric uncertainty.

[45] A non-cyber example of this relates to the case of the "DC sniper," referred to by Markle (2003). In 2002, a sniper was shooting residents of the greater Washington, DC, area for no apparent reason. At one stage, law enforcement authorities suggested that the sniper was driving a white panel van, after which point the public and state/local law enforcement appeared to focus efforts on finding white vans. The sniper was later found to have been driving a blue Caprice Classic. The inaccurate information relating to the white van directed investigative efforts in the wrong direction.

capacities increase, even machines can be overwhelmed: in cybersecurity, certain antivirus and IDS/IPS tools only allow for the simultaneous use of a fixed number of threat signatures; new signatures are either ignored or crowd out older ones. Lastly, entities who lack personnel with the skills/knowledge/training on how to best leverage shared information, or who lack the technical tools and resources to do so, may find shared information to be of little use.

As noted, homeland/national security information sharing is ubiquitous within the public and private sectors, particularly in the post-9/11 environment. Footnote 14 of the present paper provides examples of cybersecurity information sharing efforts; examples of (primarily) noncyber information sharing efforts include the Nationwide Suspicious Activity Reporting (SAR) Initiative, the national network of fusion centers, Infragard, Law Enforcement Online, and the Regional Information Sharing System, to name a few (see also the PM-ISE *Annual Report to Congress* for more discussion of specific initiatives).

But while information sharing efforts may be ubiquitous, participation in them appears to be lacking, particularly among private-sector entities. Indeed, the literature reports that participants in information sharing efforts are often reluctant to share information, particularly with the government. Such reluctance exists for a variety of reasons, including perceived or actual legal barriers (e.g., relating to collusive behavior and antitrust prohibitions, third-party liability issues, lack of authority), competitive barriers (e.g., information may be a product offering or other competitive advantage), information handling restrictions (e.g., classification or other restrictions, like "U.S.-only"), potential for reputational damage (e.g., to share price), and regulatory consequences (see, for example, White House 2009; see also Fleming and Goldstein [2011] for a brief discussion of DHS authorities in this regard). Some of this relates to trust and the proper handling of shared information (see "loss of control," above): the DHS *Information Sharing Strategy* (2008) notes that "creating a broad foundation for information sharing requires trust between all information sharing partners. Lack of trust stems from fears that shared information will not be protected adequately or used appropriately."[46] All of this is to say that information sharing as a process is not cost-free, and thus the marginal benefits of participating in an information sharing effort must exceed the marginal costs of doing so.[47]

[46] Without trust, information sharing may be unsustainable, or its maximum effectiveness may be unachievable. Partners lacking a foundation of positive interactions and corresponding personal trust withhold information, leading to a sharing "death spiral" in which fewer and fewer entities contribute information, leading to reduced trust and further limiting the willingness of participating entities to share information (see also footnote 39).

[47] Research suggests that this is not always the case, however; for example, a 2004 GAO audit of information sharing with critical infrastructure stakeholders suggested that the industry was not receiving sufficient benefit from participation: "[Industry] concerns included the limited quantity of information and the need for more specific, timely, and actionable information. In particular, one ISAC noted that it receives information from DHS simultaneously with or even after news reports, and that sometimes the news reports provide more details" (GAO 2004).

Table 3. A Definition of Information Sharing and a Summary of Its Implications for Information Sharing Performance Measurement

Definition of information sharing
Information sharing represents the process through which information is provided by one entity to one or more other entities to facilitate decision making under conditions of uncertainty, where:
▪ Information represents "data + meaning"
▪ Decision making represents goal-directed behavior in the presence of options
▪ Uncertainty represents the state of being not known, indeterminate, questionable, variable

Implications of the definition of information sharing for performance measurement
Information sharing should be goal-directed
Information should be shared with entities who can effect achievement of the goal or affect how the goal is achieved—but not with those who cannot
Shared information should be used for purposes that can effect or affect achievement of the goal—but not for purposes that cannot
Shared information should be fit for the purpose of reducing uncertainty
Information sharing cannot reduce all uncertainty, and, in some cases, it may increase it

Notes: The definition of information sharing and associated implications are used to guide the development of metrics for measuring the performance of information sharing efforts. Also, the word "goal," as used here, is synonymous with "mission." Sources: HSSAI staff, Floridi (2009), Hansson (2005), and Merriam-Webster (2002).

IV. Findings: Metrics for Critical-Infrastructure-Centric Cybersecurity Information Sharing

This chapter presents the holistic suite of metrics for measuring the performance of critical-infrastructure-centric cybersecurity information sharing efforts, heavily informed by the theoretical underpinnings on performance measurement and information sharing discussed above. Following mention of certain considerations, caveats, and sources of metrics data, the chapter provides a brief overview of the metrics at the conceptual level. It then sets forth specific metrics in outcome line categories, working backward from outcomes to outputs to processes to inputs.

A. Considerations, Caveats, and Potential Sources of Metrics Data

A number of considerations and caveats are worth noting. To begin, this chapter employs an existing information sharing effort, the aforementioned CISCP (see page 11) as a lens through which to make specific metrics recommendations. As a reminder, in the CISCP, information is shared via access to a compartment on the US-CERT website; periodic in-person or telephonic collaborative exchanges; and in-person collaboration between participants on the NCCIC floor. Participating entities (including DHS) share indicators, analytic products, best practices, and the like; they also send and receive RFIs designed to gather additional information or feedback. Despite focus on the CISCP, the findings here should be of broad relevance to other information sharing efforts as well. For example, numerous cybersecurity information sharing efforts employ websites to facilitate multilateral sharing; website-driven sharing itself differs little, fundamentally, from sharing via e-mail or Internet chat sessions, so findings here should be applicable.

Also, note that while this paper presents a first step in performance measurement, it is by no means the last. It is unrealistic to assume that metrics, once recommended, will be immediately deployed or captured. Indeed, given the broad disparity in the use and collection of metrics by entities within and outside the cybersecurity arena, it is almost certain that no turnkey approach exists. Rather, the metrics recommended here will need to be operationalized. This process will include socialization with participants; their assessment of the metrics for appropriateness, feasibility, the existence of and access to supporting data, and strategies for data capture; the setting of targets; and the collection of initial baseline data.[48] And information sharing efforts will inevitably mature over time. In this regard, it may be the case that metrics of use in the early stages of an effort—perhaps metrics that focus on ensuring an effort is functioning internally—will later become less important than those focused on ensuring that an effort is having the desired impact.[49]

Certain concepts are identified below as "evaluative" concepts. These represent concepts that should be measured once or on an as-needed basis to support more formal, more in-depth program evaluation. They are distinct from the periodically collected metrics used in performance measurement. These

[48] This process will inevitably result in the culling of certain metrics recommended here, to put greater focus on certain aspects of the information sharing effort and to minimize measurement fatigue.

[49] Along similar lines, DoD (2009) notes, in its discussion of NIST 800-55-1, that "as CS/IA [cybersecurity/ information assurance] measurement programs mature, old measures that are no longer useful can be phased out and new measures can be introduced to continue monitoring and improving the status of CS/IA." Additionally, all metrics can be "gamed" such that recorded performance exceeds actual performance. Over time, metrics could be assessed for the extent to which they appear to be too easily gamed.

evaluative concepts are included here because of their foundational relevance to measuring the efficacy of information sharing efforts, as well as their explanatory ties to other metrics concepts.

Of course, performance measurement may face certain constraints. To begin, the present paper suggests metrics for measuring the performance of information sharing efforts that cross multiple critical infrastructure sectors. But sectors will likely have different needs (and face different risks), and the cross-sector metrics proposed here need to be more generic than metrics designed to measure information sharing for specific sectors. Perhaps more importantly, because participants in these kinds of information sharing efforts may themselves be information sharing entities (like ISACs), collecting data for metrics may be difficult. This is the case because ISACs may not necessarily have direct access to data for use in metrics; rather, they will need to poll their members somehow—a step that may add cost, including data collection time (and measurement fatigue), to performance measurement. And certain metrics here may need to rely on subjective data, such as perceptions of participants, as objective data may be too difficult to obtain.

Lastly, data supporting the metrics recommended in this chapter may be pulled from three main sources: administrative records (including account logins, collaborative meeting attendance); the shared information itself; and entities participating in the effort (including DHS).[50] Data from these sources may be used in their totality (as a census, drawing on all records in a field) or in part (as a random sample pulled from a larger frame). The choice of data source and use should seek to limit measurement fatigue on the part of participating entities, to the extent possible.

B. Theoretical Underpinnings and Metrics at the Conceptual Level

What metrics should be used by critical-infrastructure-centric information sharing efforts? Metrics should measure performance in information sharing; the focus here, after all, is cybersecurity information sharing (vice cybersecurity itself).[51] Guided by first principles from the previous chapter—what is to be measured (information sharing); what is information sharing (information sharing is the process through which…); what are the implications of the definition of information sharing for performance measurement (information sharing should be goal-directed…)—an appropriate suite of metrics begins to emerge. Metrics within this suite serve to suggest 1) whether an effort itself is functioning as anticipated (internally); and 2) whether an effort is having the desired impact, in a marginal sense, over and above other existing information sharing efforts (externally). The metrics—at a conceptual level—are presented in tables 4 and 5, below. The former sets forth the metrics following from discussion of the definition of information sharing and its implications; the latter orders the metrics using an outcome line framework. The remainder of the chapter then turns concepts into specific—and interrelated—metrics.

[50] For more on measurement, though with a focus on crime, not cyber, see Fleming (2009, particularly section A of chapter III, "Measuring the Scale of Crime in General").

[51] There is a large and growing body of literature on cybersecurity metrics, particularly software/hardware and systems security metrics. Within this literature are authors critical of the ability, at present, to truly measure cybersecurity in any meaningful way (see DoD [2009] for discussion of the state of the art and associated criticism). The present paper does not resolve disagreements; importantly, its focus is not on measuring cybersecurity *per se*, but rather measuring information sharing for cybersecurity purposes. The paper's contribution is to suggest a theory-driven, holistic suite of metrics to measure performance in a cybersecurity information sharing program.

Table 4. Implications of the Definition of Information Sharing and Associated Metrics Concepts

Implication	***Metric concept***	***Metric type***
Information sharing should be goal directed	Goal is specified	Process (evaluative)
	Goal is agreed (i.e., recognized, understood, and concurred with)	Process (evaluative)
	Goal is achieved	Outcome
Information should be shared with entities who can effect or affect achievement of the goal—but not with those who cannot	Entities (and broader constituents/customers) are appropriate (with relevance, authority, responsibility, capability to act)	Process (evaluative)
	Entities are participating (sharing information: accessing website, sending and receiving information, attending collaboration events, sitting on watch floor)	Process
Shared information should be used for purposes that can effect or affect achievement of the goal—but not for purposes that cannot	Shared information is used for both tactical and strategic purposes (e.g., information is applied to cybersecurity systems; information informs resource allocation)	Output
	No loss of control (from accidental spillage, insider theft, outside unauthorized access), no associated costs (e.g., reputational damage)	Process
Shared information should be fit for the purpose of reducing uncertainty	Shared information comprises data + meaning	Input
	Shared information is relevant	Input
	Shared information is timely	Input
	Shared information is accessible	Input
	Shared information is accurate	Input
Information sharing cannot reduce all uncertainty (in some cases, it may increase it)	No information overload	Process
	Entities are sufficiently and efficiently resourced (i.e., staffed, trained, equipped)	Process

Notes: The metrics concepts that derive from the implications are occasionally overlapping. For example, "loss of control" is a function of both inappropriate entities (users) and purposes (uses; see footnote 38); it is listed under the category "uses" for analytic convenience. Also, certain concepts above represent salient one-off or occasional concepts, better suited to formal program evaluation than periodically collected metrics; this is signified in the "metric type" column via the word "evaluative." Additionally, certain concepts—"goal is specified" and "goal is agreed"—could be considered either inputs or processes (depending on vantage point); they are considered "processes" for analytic convenience. Lastly, each metric concept is represented by one or more specific metrics (discussed later in the present paper).

Table 5. Metrics Concepts in an Outcome Line Framework

Inputs	***Processes***	***Outputs***	***Outcomes***
Shared information comprises data + meaning Shared information is relevant Shared information is timely Shared information is accessible Shared information is accurate	Goal is specified (evaluative) Goal is agreed (evaluative) Entities are appropriate (with relevance, authority, responsibility, capability to act; evaluative) Entities are participating (sharing information: accessing website, sending and receiving information, attending collaboration events, sitting on watch floor) No loss of control (from accidental spillage, insider theft, outside unauthorized access), no associated costs (e.g., reputational damage) No information overload Entities are sufficiently and efficiently resourced (i.e., staffed, trained, equipped)	Shared information is used for both tactical and strategic purposes (e.g., information is applied to cybersecurity systems; information informs resource allocation)	Goal is achieved

Notes: Certain metrics concepts above represent salient one-off or occasional concepts, better suited to formal program evaluation than periodically collected metrics (identified by the word "evaluative"). Additionally, certain concepts—"goal is specified" and "goal is agreed"—could be considered either inputs or processes (depending on vantage point); they are considered "processes" for analytic convenience. Also, each metric concept is represented by one or more specific metrics (discussed later in the present paper). Finally, certain concepts, and their specific metrics, may be more important than others; all, however, contribute in some way to a holistic suite of metrics.

C. Outcome Metrics

1. Metric concept: goal is achieved. The theoretical underpinnings in the preceding chapter suggest that information sharing is carried out to achieve a goal (i.e., it must be goal-directed). So what is the goal? As noted by DHS (2011c), a notional, if somewhat repetitive, goal of a critical infrastructure cybersecurity information sharing effort is to: "promote the safety, security, and resiliency of the Nation's critical infrastructure by establishing a robust operational cyber information sharing program that measurably improves situational awareness and incident response coordination capabilities among government and CIKR owners and operators to reduce risks posed by cyber threats."[52] Essentially, this reduces to:

- "safety, security, and resiliency of critical infrastructure promoted" (end outcome);
- "cyber-related risks [to critical infrastructure] reduced" (intermediate outcome);
- "situational awareness and incident response coordination improved" (intermediate outcome); and
- "[critical-infrastructure-centric] operational cyber information sharing established" (a function of various inputs, processes, and outputs, which are discussed below).

If "promoting safety, security, and resiliency" can be fully and unambiguously achieved by "reducing cyber-related risks," then only the latter needs to be measured. As it happens, this may be the case, at least as the end outcome is written. Certainly, safety, security, and resiliency of critical infrastructure require the reduction of cyber and physical risk (i.e., not just cyber risk). But the *promotion* of safety, security, and resiliency is an incremental concept, not an absolute one, and it seems reasonable to posit that the reduction of cyber risk does, indeed, *promote*, though perhaps not fully achieve, the safety, security, and resiliency of critical infrastructure. So measurement focus here should be placed on the "reduction of cyber risk to critical infrastructure."

Similarly, it seems reasonable to assume that the "establishment of operational cyber information sharing" should lead to an "improvement in situational awareness and response coordination" (in some ways, this may be tautological, at least with situational awareness). Measurement focus should be placed on the broader and multi-faceted "establishment of critical-infrastructure-centric operational cyber information sharing," the topic of subsequent sections on input, process, and output metrics.

As such, specific metrics for the "goal is achieved" outcome concept should measure the extent to which cyber-related risks to critical infrastructure are reduced. As noted, critical infrastructure itself represents "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (USA PATRIOT Act of 2001 [42 U.S.C. 5195c Sec. 1016e]; see page 9 for more on critical infrastructure and its protection).

[52] As worded, this broad goal exhibits many layers of complexity. These derive from the definitions (and measurability, or not) of words like "promote," "robust," "measurably improves," "reduce"—and perhaps even "safety, security, and resiliency." Additionally, this CISCP goal could be strengthened in future iterations by dropping the word "promote." It is easier to achieve *promotion* of a concept than to achieve the concept itself.

The designation of critical infrastructure is based upon the *consequences* of incapacitation, exploitation, or destruction, rather than upon any inherent vulnerability in the infrastructure itself or the threat it faces.[53] In the context of cybersecurity, the consequences of greatest concern broadly represent cyber-caused unavailability of critical services (such as electricity generation, emergency medical care, potable water, etc.) and cyber-caused losses of critical data (for example, national security information or sensitive intellectual property).

Accordingly, outcome metrics should measure:

- (reductions in) critical-infrastructure-centric high-consequence cyber incidents or incidents that with time and adversary effort could become high-consequence cyber incidents (including precursor activity)—or proxies of both;[54]

- (reductions) in the damage caused by (i.e., in the consequences of) such incidents—or proxies thereof; and

- the extent to which information sharing is driving activity that should reduce likelihood and consequence of critical-infrastructure-related incidents in the future (by reducing threats, vulnerabilities, or consequences)—though this may also be measured through input, process, and output metrics.[55]

Notably, this research is focused on measuring the performance of an information sharing effort. Outcome metrics, once measured, must be *interpreted* to determine whether performance is sufficient or whether the effort is effective—that is, whether the effort is *causing*, not just correlated with, particular desired outcomes. In an ideal world, it might seem appropriate to measure information sharing, measure (high-consequence) cyber incidents or proxies and a raft of control variables, and claim success if the data suggest an increase in information sharing and a decrease in cyber incidents, *ceteris paribus*. In truth, however, it may or may not be the case that a change in cyber incidents is the result of information sharing—and interpretation of outcome data in this case is decidedly less straightforward.[56] This is because of: 1) simultaneity, as the term is called in econometrics; and 2) challenges in selecting and measuring control variables. These are addressed in turn:

[53] Risk is a function of the likelihood of an adverse event and the consequences should that event occur. The likelihood of an adverse event can be further thought of as a function of threat and vulnerability.

[54] As per NIST 800-61-1 (2008b), "a computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." Also, in the event, "lesser" cyber incidents are not of significant relevance here—unless those lesser incidents represent the early stages of incidents with potentially devastating consequences.

[55] In this regard, some metrics here are measures of good outcomes (the extent to which fewer incidents are happening or damage caused by incidents is being reduced over time), and some are measures of *precursors* to good outcomes (the extent to which fewer incidents are likely to happen in the future given changes to threat, vulnerabilities, or consequences).

[56] The problem is that it is unclear what would have happened in the absence of the information sharing effort, a concept known as the counterfactual. The counterfactual may be *estimated*, but it is by definition unknowable.

- Simultaneity exists when an independent variable is determined jointly with the dependent variable.[57] Here, cybersecurity information sharing (an independent variable) should affect cyber incidents (the dependent variable), but cyber incidents should simultaneously affect cybersecurity information sharing. More precisely, an increase in cyber incidents involving entities participating in an information sharing effort should lead to an increase in information sharing; an increase in information sharing should lead to a reduction in cyber incidents (and, subsequently, less information sharing)—or it could lead to an increase in cyber incidents because information sharing has uncovered cyber incidents that were previously unknown. Thus, isolating whether information sharing is reducing cyber incidents is no mean feat. Certain econometric methods may be used to cope with simultaneity—typically involving the use of an "instrumental variable" (a variable that exhibits a relationship with information sharing, but is not a function of rates of cyber incidents)—but these can be quite complex. In the present case, factors related to information sharing not determined by cyber incidents could include changes to the number of entities participating in an information sharing effort or changes to the information sharing behavior of existing participants. Whether such factors are easily measurable or contain enough variation over time "to tease out true relationships between variables" (Fleming 2007) is unclear.

- Further, reductions or increases in cyber incidents may result from changes in the cybersecurity environment unrelated to information sharing. For example, threat actors may choose to hack with greater verve, or though unlikely, may decide to turn away from hacking completely. Similarly, vulnerabilities may decrease through better software assurance, better patch management, stronger and more usable encryption, more effective intrusion prevention systems, and so on. Analyses seeking to isolate the impact of information sharing on cyber incidents must control for such exogenous factors. Otherwise, claims about the efficacy of information sharing may be specious. Unfortunately, many such factors are likely difficult to measure, and will be difficult to control for, particularly given that the cybersecurity environment is in a tremendous state of flux, with new technologies introduced daily or weekly.

The above serves as a reminder that 1) metrics must be interpreted with caution; and 2) as per the aforementioned balanced scorecard concept, a suite of metrics should be used in lieu of a single measure of performance. After all, though decidedly less rigorous than econometric analysis, if most or all of the metrics in the suite—from inputs to outcomes—are suggestive of good performance, then it seems reasonable to conclude that performance is good.[58] Additionally, as directed by DHS, information

[57] Considerable research on simultaneity and its implications exists. For an overview of relevance to security, see Levitt and Miles (2006) and associated references; for a brief discussion of the issue with respect to measuring the efficacy of information sharing for financial crime reduction, see Fleming (2007).

[58] Of course, this discussion has assumed that information sharing and cyber incidents are both measurable. Facets of information sharing should be measurable (the thrust of the present paper)—but cyber incidents may be less so. This is because entities may not in all cases be aware that there has been an incident in the first place (a theft of intellectual property may never be discovered, for example). Awareness is a function of, among other things, the technical capabilities of the attacked entity and of the attacker, and the type (violation of confidentiality, integrity, availability) and severity of cyber attack. Further, even if aware, attacked entities may choose to not share any information for various reasons, including fear of reputational damage, legal restrictions on sharing, and the like (see page 28). Lastly, the estimation of costs (including damages from incidents, i.e., their consequences) remains a very inexact science, and entities are unlikely to use a standard methodology; any reported cost estimates should be viewed as rough orders of magnitude at best (see footnote 3).

sharing is assumed here to be a mission need, and this research does not seek to empirically test the hypothesis that cybersecurity information sharing reduces outcomes of serious cyber incidents. Formal econometric assessment of causal achievement of outcomes could be, and should be, examined in a more in-depth program evaluation.

Bearing interpretation and measurement challenges in mind, some measures exist that can offer insight into whether the desired outcomes have been achieved.[59] **These measures, each for a given time period, include:**

a. **number of incidents causing unavailability of critical services and estimated associated costs of damage (for remediation/recovery and also due to unavailability of critical services);**

b. **number of incidents causing the loss of critical data and estimated costs of damage (for remediation/recovery and also due to loss of critical data);**

c. **more generally, total number of detected incidents, both prevented and successful, and estimated costs of damage (for remediation/recovery and also due to incidents);**

d. **unplanned downtime, in hours;**

e. **mean time to incident detection;**

f. **mean time to incident remediation;**

g. **mean time to incident recovery; and**

h. **mean time between incidents** (see the glossary, page 49, for more information on the composition of specific metrics).

D. Output Metrics

1. Metric concept: shared information is used for both tactical and strategic purposes. As noted, achievement of a goal typically requires both tactics (such as minimizing specific threats, vulnerabilities, and consequences) and strategy (including recognizing long-term trends and informing resource allocation). Tactical purposes generally fall into the broad category of deploying and improving security controls (including IDS/IPS, antivirus, logs, etc.)[60] Shared information can both inform the selection of appropriate security controls (by determining threats, associated vulnerabilities, and consequences of the greatest significance) and improve the efficacy of existing controls (by increasing the quantity and especially quality of signatures used in an IPS, for example). Shared information can also support the

[59] Numerous different metrics for measuring cyber incidents may be found in the literature, only a handful of which are presented here. The field is still evolving, and most cyber incident metrics are viewed as suboptimal for a variety of reasons. Indeed, cyber metrics, including on outcomes, are a priority area for cybersecurity research.

[60] A further discussion of critical security controls is presented by SANS (2011b), which notes that "a rational way to meet [security] requirements is to jointly establish a prioritized baseline of information security measures and controls that can be continuously monitored using automated mechanisms."

tactical evaluation of security controls by allowing baseline comparisons between similar entities.[61] Strategically, participating entities, whether public or private, must make resource-allocation decisions that reduce risk in a cost-effective manner. Shared information that demonstrates trends in cybersecurity threats or vulnerabilities can inform cost-benefit analyses to justify strategic investments in tactical cybersecurity measures. Such strategic investments might include hiring additional or different types of cybersecurity personnel, purchasing new technologies, or modifying organizational processes or policies.[62]

That shared information is used for both tactical and strategic purposes can be measured by:

a. the percentage of participating entities reporting that they use shared information to improve or implement security controls in a given time period (tactical use);

b. the percentage of participating entities reporting that they use shared information to inform resource-allocation decisions, such as those relating to strategic hiring, capital investment, and policy design, in a given time period (strategic use);

c. the percentage of received (i.e., accessed) information participants use to improve or implement security controls in a given time period (tactical use); and

d. the percentage of received (i.e., accessed) information participants use to inform resource-allocation decisions in a given time period (strategic use).[63]

These metrics can be tied to others, such as those on participation and information relevance, below, to tell a more compelling story about differences in use for more or less active participants and those who view shared information as more or less relevant. Regular metrics could be viewed alongside any in-depth program evaluation, which might also seek to capture specific examples of tactical and strategic use of shared information from participating entities.

[61] For more on evaluating the effectiveness of security controls, see NIST (2008a).

[62] NIST (2005) notes: "Determining the benefit to the agency from IT security investments is a key criterion of IT security planning. Traditionally, IT security and capital planning have been thought of as separate activities by security and capital planning practitioners. However, with FISMA legislation and existing federal regulations that charge agencies with integrating the two activities and with increased competition for limited federal budgets, agencies must effectively integrate their IT security and capital planning processes." These views apply to private sector entities as well, who face a business need to justify strategic investments in cybersecurity.

[63] Questions on specific uses of shared information could also be added to the feedback forms accompanying DHS-produced analytic products.

E. Process Metrics

1. Metric concept: goal is specified (an evaluative concept, not for regular metrics capture). Goal-directed behavior requires all entities participating in an information sharing effort to clearly understand the desired goal. Individual goals may differ between participating entities based upon their unique missions and characteristics; goals should, however, align to at least one common outcome. The presence of the goal: 1) enables a shared understanding of the benefits resulting from participation in an information sharing effort; and 2) provides a framework for measuring progress toward such benefits. The goal can be defined through consensus between participating entities, or issued from a single administering entity (such as DHS or an ISAC).

That the goal is specified can be measured by:

a. **determining whether the goal has been developed, issued, and disseminated by a coordinating body to all entities participating in the information sharing effort**.

This should be observed from both the goal originator (was the goal issued?) and the participants (was the goal received by all relevant entities?). This is more of an evaluative concept, one better suited to more in-depth (but less frequent) program evaluation than higher-level (but more frequent) performance measurement. A more in-depth evaluation might seek to assess whether the goal addresses the problem at hand, is at least theoretically achievable, and accords with (or establishes) prevailing strategy.

2. Metric concept: goal is agreed (an evaluative concept, not for regular metrics capture). By acknowledging and concurring with the goal, entities signal that they perceive value in participating in an information sharing effort. Concurrence, in turn, can promote the development of trusted relationships and can further information sharing. It can also drive the sharing of the kind of information that is fit for the purpose of achieving the goal. Concurrence can be achieved through a collaborative goal-development process or by requiring all participants to officially concur with the goal (e.g., by signing a CRADA or other governance document).

That the goal is agreed can be measured by:

a. **identifying the percentage of participating entities providing express or implied concurrence**.

As above, this is more of an evaluative concept, one better suited to program evaluation than performance measurement. A more in-depth evaluation might seek to capture the existence of and reasons for any dissent among participating entities.

3. Metric concept: entities are appropriate (an evaluative concept, not for regular metrics capture). Entities participating in a critical-infrastructure-centric cybersecurity information sharing effort should possess sufficient relevance (bearing upon the matter at hand), authority (license to make decisions), responsibility (accountability for achieving the goal), and capability to act (power to effect or affect achievement of the goal). As discussed, the goal in this case is "to promote the safety, security, and resiliency of critical infrastructure," or, more simply, "to reduce cyber-related risks to critical infrastructure." Thus, participating entities should have the ability, directly or indirectly, to reduce cyber-related risk to critical infrastructure: the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating

impact on security, national economic security, national public health or safety, or any combination of those matters." Participating entities should be in a position to provide information or analysis, or to use such information or analysis, to inform and make risk-reduction decisions. Aside from the government, participating entities could include for-profit and not-for-profit entities from industry and academia, such as specific critical infrastructure owner/operators, information sharing and analysis organizations, security application and service vendors, MSSPs, and ISPs.

That entities are appropriate in an information sharing effort can be measured by:

a. the percentage of participating entities who meet specific DHS-specified criteria; and

b. the percentage of participating entities who report that they can generate, analyze, or use information to achieve the goal.

As above, this is more of an evaluative concept, one better suited to program evaluation than performance measurement. A more in-depth evaluation might seek to examine the extent to which broader critical infrastructure assets are somehow directly or indirectly protected by participants in specific information sharing efforts. It might also assess whether criteria guiding the selection of participating entities are appropriate, transparent, and evidence-based (or at least theoretically sound). Lastly, a more in-depth evaluation could ask participating entities to identify other entities who should join the effort.

4. Metric concept: entities are participating. Appropriate entities should be participating in the critical infrastructure information sharing effort. After all, by definition, information sharing is a process that requires multiparty behavior to achieve a goal; a lack of participation calls into question the purpose of an information sharing effort in the first place. Further, information sharing is a two-way process in which participating entities both send and receive information. This sending and receiving typically occurs—using the DHS-led CISCP as an example—via access to a compartment on the US-CERT website; periodic in-person or telephonic collaborative exchanges; and in-person collaboration between participants on the NCCIC floor. Participating entities share indicators, analytic products, best practices, and the like; they also send and receive RFIs designed to gather additional information or feedback.

That entities are participating can be measured as follows:

a. the percentage of entities logging on to the information sharing website at least once in a given time period;

b. the percentage of entities sending (i.e., posting/uploading) information to the website at least once in a given time period;

c. the percentage of entities receiving information (i.e., accessing/downloading analytic products) from the website at least once in a given time period;

d. the percentage of entities participating in (i.e., calling in or attending) major scheduled collaborative exchanges in a given time period;

e. the percentage of entities with at least one person on the NCCIC floor at least once in a given time period;

f. the percentage of entities who report independent collaboration with other entities in a given time period;

g. the percentage of entities responding to RFIs (even if just to say "no information"—unless silence is viewed as concurrence) in a given time period.[64]

These would be regularly collected performance measurement metrics; in-depth evaluation would examine why participation rates are high or low and stable or increasing/decreasing over time (declining participation, for example, suggests entities perceive that the marginal costs of participation outweigh the marginal benefits).

5. Metric concept: no loss of control. Information should not be shared, purposely or accidentally, outside of the pool of appropriate entities; doing so represents a "loss of control." Loss of control violates the confidentiality and potential integrity of shared information. It incurs certain costs, such as loss of intelligence to adversaries, harm to reputations of participating entities, and weakening trust between information sharing participants. It should be minimized.

This concept is perhaps most easily measured in the negative. **That loss of control occurs can be measured by querying participating entities and DHS on:**

a. the number of loss of control events involving information from the specific information sharing effort due to cyber thefts of information (from the systems of participating entities or DHS) in a given time period;

b. the number of loss of control events involving information from the specific information sharing effort due to the theft by insiders (taken from participating entities or DHS), in a given time period;

c. the number of loss of control events involving information from the specific information sharing effort due to accidental spillage (by participating entities or DHS) in a given time period.

6. Metric concept: no information overload. Information sharing can, in certain circumstances, lead to information overload. Each piece of information sent or received entails a resource cost to entities involved. There are several reasons for this. For instance, personnel are typically required to send, receive, analyze, and deploy information. Additionally, information sharing commands network resources (including bandwidth) and storage space (including storage of threat signatures in signature files of fixed length, requiring newer signatures to potentially crowd out older ones). At a certain point—

[64] Also of interest might be measurement of the percentage of total entities who represent "free-riders," entities who frequently *receive* information but only infrequently *send* it. Additionally, certain analytic products contain brief feedback forms (also known as "customer surveys") to allow product authors to understand readers' satisfaction. These could be considered, in some sense, a type of RFI; they should also be measured. Further, along with the metrics above, it might be of use to assess the percentage of participating entities who would not be sharing information together were it not for the specific cybersecurity information sharing effort. Lastly, it might be worth tracking the number of analytic products drafted by DHS per participating entity and the ratio of the number of analytic products drafted by DHS to the number of submissions of information by participating entities in a given time period.

likely one that differs by participating entities— the marginal costs of participation outweigh the marginal benefits of doing so. That is, information sharing may reach a point of overload, after which it becomes more difficult to effect or affect achievement of the goal.[65] For example, once past the point of information overload, the integration of information into IDS/IPS might occur too slowly to prevent intrusions.

This concept is perhaps most easily measured in the negative. **That information overload exists can be measured by:**

a. **the percentage of participating entities (including DHS) reporting that the quantity of information shared exceeds their information handling and processing capability in a given time period**.

A more in-depth program evaluation would seek to understand why information overload might be occurring. This is, of course, allied to the concept of resources, below.

7. Metric concept: entities are sufficiently resourced. Effective information sharing requires that participating entities are sufficiently staffed, trained, and equipped. That is, entities need to have sufficient numbers of personnel possessing knowledge, skills, and abilities related to sharing information and putting shared information to operational use, as well as the technical tools to do so.

This concept is perhaps most easily measured in the negative. **That entities are *insufficiently* resourced (i.e., that they face resource *gaps*) can be measured by:**

a. **the percentage of participating entities (including DHS) reporting that they have insufficient *personnel* to send, receive, analyze, and deploy information;**

b. **the percentage of entities reporting that their personnel are not sufficiently *trained* to send, receive, analyze, and deploy information; and**

c. **the percentage of entities reporting that they are not *equipped* with sufficient technical tools to send, receive, analyze, and deploy information**.

A more in-depth program evaluation would seek to examine issues relating to resource gaps, perhaps by assessing participating entities against a cybersecurity information sharing maturity model of sorts.

[65] Formally, this is the point at which marginal costs for each piece of information exceed marginal benefits.

F. Input Metrics

Shared information, the inputs of an information sharing effort, should be fit for the purpose of reducing uncertainty. Using the DHS-led CISCP as an example, "shared information" refers to information submitted by participating entities to DHS, analytic products produced by DHS and accessed by participating entities, and RFIs sent between entities and DHS. This information may be shared via the US-CERT website or in-person collaboration. Metrics relating to shared information are below.

1. Metric concept: shared information comprises data + meaning. To reduce uncertainty and to inform decision making, information must provide data elements and sufficient contextual meaning to the information consumer to facilitate the use of the data elements. Shared information in cybersecurity information sharing should thus contain both data—such as a signature of sorts—and context allowing the recipient of the information to take action—such as "this signature is known hostile, add it to a list of hostile signatures to be blocked by an IPS." This is not to suggest that each and every piece of information must physically contain elements of meaning; blanket meaning could be applied to a set of information (e.g., "all of the signatures you receive from now on should be considered hostile and should be blocked").

That shared information comprises both data and meaning can be measured by:

a. **the percentage of participating entities (including DHS) reporting that shared information they receive in a given time period contains both data and contextual meaning;**

b. **the percentage of participating entities' information submissions and DHS-produced analytic products that contain both data and meaning, when examined as random samples**.

2. Metric concept: shared information is relevant. Critically, shared information should meet the needs of users (participating entities and DHS) for coverage and content.[66] That is, shared information should relate directly to the goal to be achieved, namely reducing cyber-related risks to critical infrastructure. Specifically, shared information should reduce uncertainty in decisions about critical infrastructure cybersecurity. These decisions can be tactical (e.g., "block this IP address") or strategic (e.g., "hire more security engineers"). Moreover, in informing decisions, shared information should transmit new information to its recipients—in a marginal sense, over and above information already possessed—in the form of new data, new meaning, or both.[67] An example of new data might be a novel threat signature not seen before, or at least not known about by the recipient of the information. An example of new meaning might be the fact that a known threat signature (existing data, in this case) is far more important or nefarious than previously thought, or that it is appearing in multiple (or individual but very specific) critical infrastructure sectors, indicating widespread use by threat actors. These cases might

[66] Indeed, an important, though sometimes overlooked, step in the development of any information sharing effort entails querying current and future information users on their specific information needs (i.e., their collection requirements).

[67] As it happens, one element of the concept of relevance is the extent to which information comprises both data and meaning. "Shared information comprises data + meaning" and "shared information is relevant" are treated here as distinct concepts to draw out the nuances of each.

spur DHS to issue new analytic products warning participating entities of pending trouble.[68] Indeed, repetitive receipt of previously held data, like threat signatures, might be a trigger for the creation of certain analytic products.

That shared information is relevant can be measured by:

a. **the percentage of participating entities (including DHS) reporting that the shared information they receive (separately via the website, collaborative exchanges, and the NCCIC floor) in a given time period informs decisions that reduce cyber risks to critical infrastructure;**

b. **the percentage of participating entities (including DHS) reporting that the shared information they receive (separately via the website, collaborative exchanges, and the NCCIC floor) in a given time period contains new data, new meaning, or both;**

c. **the percentage of *specific* information submissions or analytic products (not least alerts and bulletins or similar high-priority information) released in a given time period that entities report as informing decisions, and containing new data, new meaning, or both; and**

d. **for specific submissions or products that were not yet known about, the number of instances in a given time period that the shared information, once deployed, led to the discovery of a previously unknown cyber incident (including, if possible, any damage caused by the incident)**.[69]

Responses may differ significantly between participating entities, as the previously held information identified by a particular entity will depend in part upon the quantity (and quality) of information already possessed by that entity. The fact that specific participating entities already possess information does not undermine the entire utility of an information sharing effort if the effort successfully transmits new information to at least certain other entities.

3. Metric concept: shared information is timely. Cyber-related risk is ever changing, as cyber threats are eminently adaptable and new technologies with new vulnerabilities are introduced daily. The more time between information origination (e.g., discovery of a new hostile signature or vulnerability) and broad receipt by entities participating in an information sharing effort, the more harm cyber threats can cause before cyber defenders act.[70] Thus, to usefully inform cybersecurity decision making—to reduce

[68] Of course, repetitive receipt of previously held data becomes less relevant when the marginal benefit bestowed by new meaning is exceeded by analytic and processing cost (see the discussion of information overload, above). Along these lines, an information sharing effort is most useful precisely for its dissemination of novel information; as the amount of novel information declines, entities may see less value in continued participation.

[69] For completeness, that shared information is relevant can also be measured by: 1) the percentage of information received (separately via the website, collaborative exchanges, and the NCCIC floor) by participating entities (including DHS) in a given time period that informs decisions that reduce cyber risks to critical infrastructure; 2) the percentage of information received (separately via the website, collaborative exchanges, and the NCCIC floor) by participating entities (including DHS) in a given time period that contains new data, new meaning, or both. These overlap in part, at least theoretically, with metrics suggested above for outputs. Separately, analytic products sometimes include feedback forms to gauge customer satisfaction; these might serve useful in assessing the relevance of specific products.

[70] Certain cybersecurity information is considered "perishable" if not shared in a timely fashion.

uncertainty therein—shared cybersecurity information should be current, shared as close as possible to the period to which the information refers. This is true for entities reporting threat and vulnerability information as well as analysts responsible for developing and disseminating analytic products.

That shared information is timely can be measured by:

a. **the percentage of participating entities (including DHS) reporting that shared information is received in sufficient time to support the goal;**

b. **the percentage of DHS-produced analytic products meeting timeliness targets for production (particularly alerts and bulletins); and**

c. **the percentage of RFIs responded to within timeliness targets (particularly RFIs relating to alerts and bulletins).**

4. Metric concept: shared information is accessible. For shared information to be of use in decision making (and uncertainty reduction), it must be accessible to participating entities. Otherwise, participating entities may find that the marginal cost of retrieving and preprocessing shared information exceeds the marginal benefit of its use. Accordingly, shared information must be: 1) available (e.g., the information sharing website should be running, users should be able to log in, and information should be easily navigable; collaborative events should be scheduled in advance and located to mutual benefit, to the extent possible; there should be no barriers entry on the NCCIC floor); and 2) formatted for convenient and immediate use (e.g., machine-readable or sufficiently straightforward).

That shared information is accessible can be measured by:

a. **the percentage of participating entities reporting that the information sharing website is consistently up and running, with no login issues;**

b. **the percentage of participating entities reporting that accessing and locating information on the website is straightforward; and**

c. **the percentage of participating entities reporting that converting received information to operational utility is straightforward**.[71]

For more granularity, **that shared information is accessible can also be measured by:**

d. **the percentage of time in a given time period that the information sharing website is unavailable (down, for whatever reason); and**

e. **the number of website login issues reported to DHS by participating entities in a given time period**.[72]

---

[71] Improving the accessibility of information for machine-to-machine sharing requires use of a common framework or taxonomy.

5. Metric concept: shared information is accurate. Shared information should be as close as possible to the (unknown) true value. This is because the sharing of inaccurate information—inaccurate data, inaccurate meaning, or both—does not reduce uncertainty. Indeed, it may impose costs on entities participating in an information sharing effort by consuming analytic resources.[73] It may also reduce trust in the value of shared information.[74]

That shared information is accurate can be measured by:

a. the number of unique instances of inaccurate information reported by participating entities (including DHS) in a given time period.

It is expected that instances of inaccuracy will be low, not least because determining accuracy may require more confirmatory or contradictory information than is (easily) available.

G. Descriptive Statistics

In addition to the metrics described above—in some cases to facilitate their production, or to explain their findings—certain descriptive statistics should be captured at regular intervals. These include the following:

- Number of entities participating in the information sharing effort. This measurement could be categorized by progress in the on-boarding process—from initial discussion to full participation—and also by critical infrastructure sector (though certain participating entities will relate to multiple sectors).
- Size (annual revenue or similar) and annual cybersecurity budget (if possible) of each entity.
- Number of full-time-equivalent (FTE) staff dedicated to the information sharing effort by DHS and by each participating entity.
- Annual expenditure, per participating entity, excluding FTE (e.g., on technology) to support the information sharing effort.
- Number of days required to on-board each participating entity (between identification of appropriate entity and accession to full participation, as judged by access to the website).
- Number of information submissions sent to the website by each participating entity (and total for all entities) in a given time period.

---

[72] To access information, participating entities typically complete an on-boarding process that includes signing legal agreements governing participation. Anecdotal information suggests that this process can be lengthy. It could be useful to track time required for on-boarding to monitor for what appear to be undue delays or increases in on-boarding time.

[73] When an entity receives information, it must consider whether information should be employed/deployed, included in an analytic product, or ignored. Inaccurate information makes this decision more difficult and could lead to two suboptimal possibilities: true information mistakenly rejected as false (a type 1 error) or false information incorrectly accepted as true (a type 2 error; Weiss 2006). See also Perry and Moffat (2004) for a more quantitative discussion of accuracy and decision making in information sharing.

[74] Accuracy relates to concepts of bias and precision. With an unbiased estimator, the expected value of a parameter equals its true value ($\hat{\mu} = \mu$). Precision refers to consistency of repeated measurements taken under identical conditions (Taylor 1997).

- Number of unique signatures (indicators) collected by DHS via the information sharing effort in a given time period.
- Number of DHS products released, categorized by product type, in a given time period.
- Number of hours used by DHS to produce each product, by product type (from information submission to product posting).
- Number of hours between product posting and entities' downloading/accessing product.
- Number of DHS products downloaded (or otherwise accessed) by product type in a given time period.
- Number of RFIs sent, and number received (and number of DHS product feedback forms received containing feedback) in a given time period.
- Number of specific scheduled group collaboration events (conference calls and group meetings) in a given time period.

H. Summary

In sum, a suite of interrelated metrics should be used to measure the efficacy of critical-infrastructure-centric cybersecurity information sharing efforts. These are summarized in table 6.

Table 6. Metrics for Measuring the Performance of Critical-Infrastructure-Centric Cybersecurity Information Sharing

Inputs	*Processes*	*Outputs*	*Outcomes*
Shared information comprises both data and meaning: ▪ % of participating entities reporting that shared information received in a given time period contains both data and meaning ▪ % of submitted information and analytic products (based upon a random sample) that contain both data and meaning **Shared information is relevant:** ▪ % of participating entities reporting that the shared information they receive in a given time period informs decisions that reduce cyber risks to critical infrastructure ▪ % of participating entities reporting that the shared information they receive in a given time period contains new data, new meaning, or both ▪ % of *specific* information submissions or analytic products released in a given time period that inform decisions, and contain new data, new meaning, or both ▪ Number of instances in a given time period that *specific* submissions or products that were not yet known about led to the discovery of a previously unknown cyber incident, once deployed	**The goal is specified:** ▪ % of participating entities reporting that the goal has been developed, issued, and disseminated by a coordinating body **The goal is agreed upon:** ▪ % of participating entities providing express or implied concurrence with goal **Participating entities are appropriate:** ▪ % of participating entities who meet specified criteria ▪ % of participating entities who report that they can generate, analyze, or use information to achieve the goal **Entities are participating:** ▪ % of entities logging on to the information sharing website at least once in a given time period ▪ % of entities sending information to the website at least once in a given time period ▪ % of entities receiving information from the website at least once in a given time period ▪ % of entities participating in scheduled collaborative exchanges in a given time period ▪ % of entities with at least one person on the NCCIC floor at least once in a given time period ▪ % of entities who report independent collaboration with other entities in a given time period ▪ % of entities responding to RFIs in a given time period	**Information is used for tactical and strategic purposes:** ▪ % of participating entities reporting use of shared information to improve or implement security controls in a given time period (tactical use) ▪ % of participating entities reporting use of shared information to inform resource allocation decisions in a given time period (strategic use) ▪ % of received (i.e., accessed) information used to improve or implement security controls in a given time period (tactical use) ▪ % of received (i.e., accessed) information used to inform resource allocation decisions (strategic use)	**Goal is achieved** (all in a given time period)**:** ▪ Number of incidents causing unavailability of critical services and estimated associated costs of damage ▪ Number of incidents causing the loss of critical data and estimated costs of damage ▪ Number of detected incidents, both prevented and successful, and estimated costs of damage ▪ Unplanned downtime ▪ Mean time to incident detection ▪ Mean time to incident remediation ▪ Mean time to incident recovery ▪ Mean time between failures

Table 6. Metrics for Measuring the Performance of Critical-Infrastructure-Centric Cybersecurity Information Sharing (continued)

Inputs	*Processes*	*Outputs*	*Outcomes*
Shared information is timely: ▪ % of participating entities reporting that shared information is received in sufficient time to support the goal ▪ % of analytic products meeting timeliness targets for production ▪ % of RFIs responded to within timeliness targets **Shared information is accessible:** ▪ % of participating entities reporting that the information sharing website is consistently up and running ▪ % of participating entities reporting that accessing and locating information on the website is straightforward ▪ % of participating entities reporting that converting received information to operational utility is straightforward ▪ % of time in a given time period that the information sharing website is unavailable ▪ Number of website login issues reported by participating entities in a given time period **Shared information is accurate:** ▪ Number of unique instances of inaccurate information reported by participating entities (including DHS) in a given time period	**Loss of control events are occurring:** ▪ Number of loss of control events involving information from the specific information sharing effort due to cyber thefts of information in a given time period ▪ Number of loss of control events involving information from the specific information sharing effort due to the theft by insiders in a given time period ▪ Number of loss of control events involving information from the specific information sharing effort due to accidental spillage in a given time period **Information overload exists:** ▪ % of participating entities reporting that the quantity of information shared exceeds their information handling and processing capability in a given time period **Entities are *insufficiently* resourced:** ▪ % of participating entities reporting that they have insufficient *personnel* to send, receive, analyze, and deploy information ▪ % of participating entities reporting that their personnel are not sufficiently *trained* to send, receive, analyze, and deploy information ▪ % of participating entities reporting that they are not *equipped* with sufficient technical tools to send, receive, analyze, and deploy information		

Notes: These metrics will need to be operationalized, a process that includes entities' assessment of the metrics for appropriateness, feasibility, the existence of and likely easy access to supporting data. It also includes developing strategies for data capture, setting targets, and collecting initial baseline data.

V. Conclusions, Next Steps, and Thoughts for Future Research

This paper presented a suite of metrics for use by DHS and others in measuring the performance of (DHS-led) critical-infrastructure-centric cybersecurity information sharing efforts. The metrics were derived through examination of theoretical underpinnings on both performance measurement and information sharing.

The suite of metrics suggested in this paper has not yet been operationalized, of course, and several next steps should be taken. These include socialization of metrics with participating entities. That process involves asking entities to assess the metrics for appropriateness, feasibility, and the existence of and likely easy access to supporting data. It also involves developing strategies for data capture, setting targets, collecting initial baseline data, and the testing of the suite of metrics in an operational setting. And once the suite of metrics is operationalized, the performance of select information sharing efforts should be evaluated—using metrics and other sources of information—at periodic intervals (perhaps yearly).

Lastly, notable avenues for future research exist. For example, critical-infrastructure-centric information sharing efforts comprise various entities. What is not clear is the extent to which broader critical infrastructure assets are somehow directly or indirectly protected via these efforts and their pool of participating entities. Future research could examine the membership and the coverage of critical infrastructure protection achieved, in theory or in practice, through various efforts. This strand of research would seek to determine whether membership could be modified to include other entities who might more effectively or more efficiently reach a sweeping swath of critical infrastructure assets. Further, multiple cybersecurity information sharing efforts persist. Future research could document and assess the existence of multiple overlapping efforts and their impact on the each other. This strand of research would seek to understand whether certain overlapping efforts should be merged, expanded, or perhaps even scaled back to reduce duplication of effort and confusion among participating entities. Along these lines, future research could also explore the numerous current (and pending) relationships that exist between various DHS elements and entities in industry, academia, and the not-for-profit worlds. This strand of research would seek to recommend best practices and procedures for strategic relationship management, to ensure that DHS speaks (and listens) to non-governmental partners with one voice.

Glossary

Term	*Definition*	*Source*
Accessibility	Information is available and easily usable (formatted for convenient and immediate use)	Fleming (2009), citing UK Office of National Statistics (ONS; 2005)
Accuracy	The closeness between an estimated result and the (unknown) true value	Fleming (2009), citing UK ONS (2005)
Coherence	The degree to which data that are derived from different sources or methods, but which refer to the same phenomenon, are similar	Fleming (2009), citing UK Office of National Statistics (2005)
Comparability	The degree to which data can be compared over time and domain	Fleming (2009), citing UK ONS (2005)
Critical infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters	USA PATRIOT Act of 2001
Cybersecurity	The full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure	White House (2009)
Cyberspace	The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people	White House (2009), citing NSPD-54/HSPD-23
Decision making	Goal-directed behavior in the presence of options	Hansson (2005)
Information	Data + meaning	Floridi (2009)
Information sharing	The process through which information is provided by one entity to one or more other entities to facilitate decision-making under conditions of uncertainty	HSSAI staff
Inputs	Resources invested into the program or activity being measured, such as funds, employee-hours, or raw materials	Hatry (2006)
Loss of control	Sharing with inappropriate entities (i.e., unauthorized users) and sharing for inappropriate purposes (i.e., unauthorized uses)	HSSAI staff

Mean time between failures	Information security metric calculated by the total uptime (during which all services/networks/data are available) divided by the total number of unplanned outages in a given time period	Adapted from Jaquith (2007)
Mean time to incident detection	Information security metric calculated by subtracting the estimated date/time of incident occurrence from the date/time of incident discovery, averaged across the number of total incidents detected	Adapted from DHS (2011b)
Mean time to incident recovery	Information security metric calculated by dividing the difference between the date/time of occurrence and the date/time of recovery for each incident recovered in a given time period, by the total number of incidents recovered in a given time period	Adapted from DHS (2011b)
Mean time to incident remediation	Information security metric calculated by dividing the difference between the date/time of occurrence and the date/time of remediation for each incident in a given time period, by the total number of incidents in a given time period	Adapted from DHS (2011b)
Outcome line	A graphical representation of the hypothesized causal chain leading from inputs (on the left) to outcomes (on the right); once fully specified, an outcome line helps to clarify: 1) what is expected to result from X (inputs and processes); and 2) how Y (the outcome of interest) can be expected to follow from X	Mohr (1995)
Outcomes	Events, occurrences or changes in condition that indicate programmatic progress, brought about at least in part through outputs	Hatry (2006)
Outputs	Completed or delivered products or services generated through inputs	Hatry (2006)
Performance management	The use of performance information to affect programs, policies, or any other organization actions aimed at maximizing the benefits of public services	Hatry (2003)
Performance measurement	Regular measurement of the results (outcomes) and efficiency of services or programs	Hatry (2006)
Processes	The steps that turn inputs into outputs	Hatry (2006)
Relevance	The degree to which the product meets user needs for both coverage and content	Fleming (2009), citing UK ONS (2005)
Timeliness	Information is current (it should be released as close as possible to the period to which the information refers)	Fleming (2009), citing UK ONS (2005)
Uncertainty	The state of being not known, indeterminate, questionable, variable	Adapted from Merriam-Webster (2002)

References

Bayuk, Jennifer L. 2011. *Measuring Systems Security: An Initial Security Theoretical Construct Framework*. PhD dissertation, Stevens Institute of Technology.

Bayuk, Jennifer L., and Barry M. Horowitz. 2011. "An Architectural Systems Engineering Methodology for Addressing Cyber Security." *Systems Engineering* 14: 294–304.

Behn, Robert. 2007a. "Danger of Using Too Few Measures." *Bob Behn's Public Management Report*. Cambridge, MA: Harvard University.

———. 2007b. "Only a Very Few Priority Measures." *Bob Behn's Public Management Report*. Cambridge, MA: Harvard University.

———. 2003. "Why Measure Performance? Different Purposes Require Different Measures." *Public Administration Review* 63: 585-606.

Campbell, Donald T., and Julian C. Stanley. 1966. *Experimental and Quasi-Experimental Designs for Research.* Florence, KY: Wadsworth Publishing.

Cashell, Brian et al. 2004. *The Economic Impact of Cyber-Attacks.* Washington, DC: Congressional Research Service.

Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency. 2011. *Cybersecurity Two Years Later*. Washington, DC: CSIS.

———. 2008. *Securing Cyberspace for the 44th Presidency*. Washington, DC: CSIS.

Cook, Thomas, and Donald Campbell. 1979. *Quasi-Experimentation: Design and Analysis Issues for Field Settings.* New York: Houghton Mifflin.

The Cybersecurity Act of 2012, S. 2150.

The Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523.

Department of Defense (DoD). 2011. *About DCISE*. Accessed 6 December 2011. http://www.dc3.mil/dcise/dciseAbout.php.

———. 2010. *Quadrennial Defense Review.* Washington, DC: DoD.

———. 2009. *Measuring Cybersecurity and Information Assurance.* Washington, DC: DoD Information Assurance Technology Analysis Center.

———. 2008. *National Defense Strategy*. Washington, DC: DoD.

———. 2007. *Information Sharing Strategy.* Washington, DC: DoD.

Department of Homeland Security (DHS). 2011a. *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise.* Washington, DC: DHS.

———. 2011b. *Chief Information Officer Federal Information Security Management Act Reporting Metrics*. Washington, DC: DHS.

———. 2011c. "CISCP Data Sharing Among Government Agencies." Washington, DC: DHS (unpublished document).

———. 2011d. "CICPA Overview of Cyber Data Flow." Washington, DC: DHS (unpublished document).

———. 2011e. "CISCP Proposed Path Forward for the Homeland Security Cyber Enterprise Environment." Washington, DC: DHS (unpublished document).

———. 2011f. "CISCP Private Sector Participation Criteria." Washington, DC: DHS (unpublished document).

———. 2011g. "Cooperative Research and Development Agreement (CRADA)." Washington, DC: DHS (unpublished document).

———. 2011h. *Enabling Distributed Security in Cyberspace.* Washington, DC: DHS.

———. 2011i. "Industrial Control Systems Cyber Emergency Response Team." Accessed 6 December 2011. http://www.us-cert.gov/control_systems/ics-cert/more_information.html.

———. 2011j. "State and Major Urban Area Fusion Centers." Accessed 6 December 2011. http://www.dhs.gov/files/programs/gc_1156877184684.shtm .

———. 2011k. "US-CERT." Washington, DC: DHS. Accessed 6 December 2011. http://www.us-cert.gov/aboutus.html.

———. 2010a. *Bottom-Up Review Report*. Washington, DC: DHS.

———. 2010b. *Information Technology Sector Specific Plan.* Washington, DC: DHS.

———. 2010c. *Quadrennial Homeland Security Review*. Washington, DC: DHS.

———. 2009a. *National Infrastructure Protection Plan*. Washington, DC: DHS.

———. 2009b. *NIPP Newsletter.* Issue 41. Accessed 6 December 2011. http://www.fbiic.gov/public/2009/march/DHS_NIPP_Newsletter_Mar09.pdf.

———. 2009c. "Secretary Napolitano Opens New Cybersecurity and Communications Integration Center." Accessed 6 February 2012. http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm.

———. 2008. *Information Sharing Strategy.* Washington, DC: DHS.

Department of Energy (DoE). 1996. *Guidelines for Performance Measurement.* Washington, DC: DoE.

Department of Justice (DOJ). 2010. *Nationwide SAR Initiative Annual Report.* Washington, DC: DOJ.

Edmunds, Angela, and Anne Morris. 2000. "The problem of information overload in business organizations: a review of the literature." *International Journal of Information Management* 20: 17-28.

Falliere, Nicholas, Liam Murchu, and Eric Chien. 2011. *W32 Stuxnet Dossier.* Accessed 20 April 2011. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Federal Bureau of Investigation (FBI). 2011. *About Infragard*. Accessed 9 January 2012. http://www.infragard.net/about.php?mn=1&sm=1-0.

———. 2011a. *National Information Sharing Strategy.* Washington, DC: FBI.

Federal Information Security Management Act of 2002, 44 *U.S.C.,* §§3543, 3546, and 11331.

Federal Technology Transfer Act of 1986, 15 U.S.C. §3710.

Fleming, Matthew H. 2009. *The Scale and Impact of Financial Crime.* London, U.K.: Financial Services Authority.

———. 2007. "Issues in measuring the efficacy of a suspicious activity reports (SARs) regime." *Amicus Curiae* 70: 9-12.

Fleming, Matthew H., and Eric Goldstein. 2011. *An Analysis of the Primary Authorities Supporting and Governing the Efforts of the Department of Homeland Security to Secure the Cyberspace of the United States.* Arlington, VA: Homeland Security Studies and Analysis Institute.

Floridi, Luciano. 2011. *The Philosophy of Information*. Oxford: Oxford University Press.

———. 2010. *Information: A Very Short Introduction*. Oxford: Oxford University Press.

———. 2009. "Philosophical Conceptions of Information." *Formal Theories of Information*. Berlin: Springer-Verlag.

Forsythe, Dallas, ed. 2001. *Quicker, Better, Cheaper: Managing Performance in American Government.* Albany, NY: Rockefeller Institute Press.

Government Accountability Office. 2008. *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*. Washington, DC: GAO.

———. 2006. *The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*. Washington, DC: GAO.

———. 2004. *Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors.* Washington, DC: GAO.

———. 2001. "Reports on the Government Performance and Accountability Act." Washington, DC: GAO. Accessed 12 March 2012. http://www.gao.gov/new.items/gpra/gpra.htm.

Government Performance and Results Act of 1993, 5 *U.S.C.,* §306.

Granger Morgan, M., and Max Henrion. 1992. *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis.* Cambridge, UK: Cambridge University Press.

Gross, Michael Joseph. 2011. "A Declaration of Cyber War." *Vanity Fair*, April.

Hansson, Sven. 2005. *Decision Theory: Brief Introduction*. Stockholm, Sweden: Royal Institute of Technology.

Hatry, Harry. 2006. *Performance Measurement: Getting Results, Second Edition.* Washington, DC: Urban Institute Press.

———. 2003. *Key Steps in Outcome Management.* Washington, DC: Urban Institute Press.

———. 1980. "Performance Measurement Principles and Techniques: An Overview for Local Government." *Public Productivity Review* 4: 312-339.

Homeland Security Act of 2002, Public Law 107-296, Title II.

Jaquith, Andrew. 2007. *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Upper Saddle River, NJ: Addison-Wesley.

Kaplan, Robert. 2010. *Conceptual Foundations of the Balanced Scorecard.* Cambridge, MA: Harvard Business School Working Paper 10-074.

———. 2001. "Strategic Performance Measurement and Management in Nonprofit Organizations." *Nonprofit Management and Leadership* 11: 353-370.

Kaplan, Robert, and David Norton. 1992. "The Balanced Scorecard: Measures that Drive Performance." *Harvard Business Review.* Jan–Feb: 71–80.

Levitt, Steven D., and Thomas J. Miles. 2006. "Economic Contributions to the Understanding of Crime." *Annual Review of Law and Social Science* 2: 147-64.

Macauley, Molly. 2005. *Some Dimensions of the Value of Weather Information: General Principles and a Taxonomy of Empirical Approaches.* Washington, DC: Resources for the Future.

Markle Foundation. 2003. *Creating a Trusted Network for Homeland Security.* New York, NY: Markle Foundation.

———. 2002. *Protecting America's Freedom in the Information Age.* New York, NY: Markle Foundation.

Masters, Jonathan. 2011. “Backgrounder: Confronting the Cyber Threat.” Council on Foreign Relations. Accessed 10 April 2011. http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577.

Merriam-Webster. 2002. *Webster's Third New International Dictionary, Unabridged*. Accessed 16 March 2012. http://unabridged.merriam-webster.com.

Mohr, Lawrence B. 1995. *Impact Analysis for Program Evaluation.* Newbury Park, CA: Sage Publications.

Moore, Mark H. 2003. *The Public Value Scorecard: A Rejoinder and an Alternative to "Strategic Performance Measurement and Management in Non-Profit Organizations" by Robert Kaplan.* Cambridge, MA: Harvard University.

National Cyber-Forensics & Training Alliance (NCFTA). “About NCTFA.” Accessed 12 January 2012. http://www.ncfta.net/about-ncfta.

National Institute of Standards and Technology (NIST). 2010. *Special Publication 800-53: Recommended Security Controls for Federal Information Systems and Organizations (Amended).* Washington, DC: NIST.

———. 2008a. *Special Publication 800-55-1: Performance Measurement Guide for Information Security*. Washington, DC: NIST.

———. 2008b. *Special Publication 800-61-1: Computer Security Incident Handling Guide*. Washington, DC: NIST.

———. 2005. *Special Publication 800-65: Integrating IT Security into the Capital Planning and Investment Control Process.* Gaithersburg, MD: NIST.

National Security Telecommunications Advisory Committee. 2010. *Network Security Information Exchanges.* Accessed 16 March 2012. http://www.ncs.gov/nstac/reports/fact_sheet/NSTAC_08.pdf.

Office of the Director of National Intelligence. 2009. *National Intelligence Strategy.* Washington, DC: ODNI.

———. 2008. *United States Intelligence Community Information Sharing Strategy.* Washington, DC: ODNI.

Office of Management and Budget (OMB). 2011. *Circular No. A-11, Part 6: Preparation and Submission of Strategic Plans.* Washington, DC: OMB.

Oak Ridge Associated Universities. 1995. *How to Measure Performance: A Handbook of Tools and Techniques.* Accessed 12 January 2012. http://www.orau.gov/pbm/documents/handbook1.html.

Otto, Boris, Martin Ofner, and Kai M. Huener. 2009. "Dealing with Complexity: A Method to Adapt and Implement a Maturity Model for Corporate Data Quality Management." *Proceedings of the 15th Americas Conference on Information Systems.*

Office of the Program Manager—Information Sharing Environment. 2011. *Annual Report to Congress.* Washington, DC: PM-ISE.

———. 2006. *PM-ISE Implementation Plan.* Washington, DC: PM-ISE.

Perry, Walter L., and James Moffat. 2004. *Information Sharing Among Military Headquarters: The Effects on Decision Making.* Santa Monica, CA: RAND Corporation.

Rossi, Peter H., and Howard H. Freeman. 2004. *Evaluation: A Systematic Approach 7th ed.* Newbury Park, CA: Sage Publications.

———. 1993. *Evaluation: A Systematic Approach 6th ed.* Newbury Park, CA: Sage Publications.

Rosenzweig, Paul. 2011. *Cybersecurity, the Public/Private "Partnership," and Public Goods.* Palo Alto, CA: Hoover Institution.

SANS. 2011. "About the Internet Storm Center." Accessed 6 December 2011. http://isc.sans.org/about.html.

———. 2011b. *Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines.* Accessed 3 March 2012. http://www.sans.org/critical-security-controls/cag3_1.pdf

The Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012, S. 2150.

Shannon, Claude. 1948. "A Mathematical Theory of Communication." *Bell System Technical Journal* 27: 379-423.

Taylor, John. 1997. *An Introduction to Error Analysis.* Sausalito, CA: University Science Books.

USA PATRIOT Act as amended, 2008, Public Law 107-56. Title V, §§ 504, 505, 506, and Title VII.

U.S. House of Representatives Republican Cybersecurity Task Force. *Recommendations.* Washington, DC: 2011. Accessed 15 March 2012. http://thornberry.house.gov/UploadedFiles/CSTF_Final_Recommendations.pdf.

Weiner, Norbert. 1950. "Entropy and information." *Proceedings of Symbolic Applied Mathematics* 2: 89-101.

Weiss, Neil. 2006. *Introductory Statistics.* San Francisco, CA: Pearson Addison Wesley.

The White House. 2010. *National Security Strategy*. Washington, DC: The White House.

———. 2009. *Cyberspace Policy Review*. Washington, DC: The White House.

———. 2007. *NSPD-54/HSPD-23: Cybersecurity Policy (unclassified summary).*

———. 2007a. *National Strategy for Homeland Security.* Washington, DC: The White House.

———. 2007b. *National Strategy for Information Sharing.* Washington, DC: The White House.

———. 2003. *HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection.*

———. 1999. *Presidential Decision Directive-63: Critical Infrastructure Protection.*

Wand, Yair, and Richard Y. Wang. 1996. "Anchoring Data Quality Dimensions in Ontological Foundations." *Communications of the ACM*. 86-95.

Wang, Richard Y., and Diane M. Strong. 1996. "Beyond Accuracy: What Data Quality Means to Data Consumers." *Journal of Management Information Systems* 12: 4.