Cross-Sector Roadmap for Cybersecurity of Control Systems

September 30, 2011

Prepared by
The ICSJWG Roadmap Working Group

Version	**Date**
1.0	**3/24/2010**
1.1	**6/10/2010**
1.2	**8/6/2010**
1.3	**8/17/2010**
1.4	**9/13/2010**
1.5	**9/27/2010**
2.0	**11/16/2010**
2.1	**1/13/2011**
2.2	**4/6/2011**
2.3	**5/31/2011**
3.0	**9/30/2011**

PREAMBLE

This Cross-Sector Roadmap was conceived and developed over the last two years by industry and government thought leaders that saw the need for a unifying Roadmap to secure control systems across all critical sectors. They have succeeded in capturing the common elements of securing control systems from the many Roadmaps that have been developed by individual sectors over the last six years. However, unifying does not mean "one size fits all" and the crafters of this Cross-Sector Roadmap hope that other critical sectors that have not developed their own Roadmap to date will either use this document as is or use it as a starting point to develop their own brand of Roadmap to secure control systems that reflects their sector's unique needs and challenges.

FOREWORD

The Cross-Sector Roadmap to Secure Control Systems describes a plan for voluntarily improving cybersecurity across all critical infrastructure/key resources (CIKR's) that employ industrial control systems. This roadmap provides an opportunity for industry experts to offer input concerning the state of control systems cybersecurity and to communicate recommended strategies for improvement. This roadmap brings together various sector stakeholders, government agencies, and asset owners and operators, with a common set of goals and objectives. It also provides milestones to focus specific efforts and activities for achieving the goals and addressing control system's most urgent challenges, longer-term needs, and practices for improvement.

The U.S. Department of Homeland Security's National Cybersecurity Division (NCSD) facilitated the development of this roadmap, with volunteers from the Industrial Control Systems Joint Working Group (ICSJWG) and industry stakeholder organizations. This roadmap provides a beginning point and a template for action as industry and government work together to achieve a common objective for securing industrial control systems (ICSs) across all CIKR's that employ ICSs.

All activities within this Roadmap should be conducted in accordance with applicable laws and policies. Nothing in this Roadmap should be taken to restrict, supersede, or otherwise replace the legal authorities or regulatory responsibilities of any government agency or organization. The views expressed within this Roadmap are those of the members of the ICSJWG Roadmap Working Group and do not constitute an official agency or organization position.

ICS ROADMAP WORKING GROUP

Name	**Organization**	**Role**
Perry Pederson	Nuclear Regulatory Commission	Co-Chair (GCC)
Tim Roxey	North American Electric Reliability Corporation	Co-Chair (SCC)
Jeff Gray	Department of Homeland Security	ICSJWG Program Lead
Lisa Kaiser	Department of Homeland Security	ICSJWG Liaison
John Zurcher	SRA International, Inc.	ICSJWG Support
Chris Scholbe	SRA International, Inc.	ICSJWG Support
Donald Allen	DHS/TSA/Mass Transit	Member
Larry Alls	GE Energy	Member
Thomas Asojo	USAF/38 CEG	Member
Matt Bailey	Fox Guard Solutions	Member
Doron Becker	Department of the Navy	Member
Sandra Bittner	Arizona Public Service Company / Palo Verde Nuclear Generating Station	Member
Chris Blask	AlienVault	Member
Mark Bodily	Idaho National Laboratory	Member
Lloyd Brake	Naval Surface Warfare Center	Member
Chet Braun	Navy NAVFAC NW	Member
Jim Brenton	ERCOT	Member
Fabien Briere	TOTAL France	Member
Tim Burkhalter	Deaf Smith Electric Cooperative, Inc.	Member
Edwin Cadag	Guam Power Authority	Member

Name	**Organization**	**Role**
Larry Camm	Schweitzer Engineering Laboratories, Inc.	Member
Eric Cosman	Dow Chemical Company	Member
Jeffrey Crabtree	Midwest Reliability Organization	Member
Ed Crawford	Chevron	Member
David DeGroot	Austin Energy	Member
Tom Dion	Department of Homeland Security	Member
John Duronio	Emerson Process Management	Member
Kevin Eberharter	Manitoba Hydro	Member
Jerome Farquharson	Burns & McDonnell Engineering	Member
William Fletcher	ICF International	Member
Thomas Flowers	CCS/EPRI	Member
John Fridye	ABB	Member
Clifford Glantz	Pacific Northwest National Laboratory	Member
Tim Grayson	Ktech Corporation	Member
Kevin Harnett	Department of Transportation/Volpe Center	Member
Ricky Hill	Tenacity Solutions, Inc.	Member
Jamey Hilleary	Elecsys Corporation	Member
Stephen Hilt	Tennessee Valley Authority	Member
Scott Hudson	Fox Guard Solutions	Member
Dawn Johnson	Department of Transportation/Volpe Center	Member
Andrew Jurbergs	Tennessee Valley Authority	Member
Pan Kamal	Alert Enterprise	Member
Bill Kim	Independence Power and Light	Member
Wade Kirschner	Department of Homeland Security	Member
Esther Langer	Department of Homeland Security	Member
Joel Langill	Englobal Automation Group	Member
Annabelle Lee	Electric Power Research Institute	Member
Brian Lenane	SRA International, Inc.	Member
Larry Lendo	Elecsys Corporation	Member
Edward Liebig	Computer Sciences Corporation	Member
James Loughlin	Owl Computing Technologies, Inc.	Member
John Lujan	Elecsys Corporation	Member
Eric Lynch	Public Works Department Kitsap	Member
David Martin	Department of Homeland Security	Member
Neil Martin	Huntsman Corporation	Member
Dan Mathis	Department of the Navy	Member
Rob McComber	Telvent USA	Member
Joe McCormick	Boeing Energy	Member
William McNaught	Idaho National Laboratory	Member
Itoro Meshioye	OSIsoft	Member
Byung-Gil Min	ETRI	Member
Ben Miron	General Electric	Member
Rene Moreda	Invensys	Member
Dude Neergaard	Oak Ridge National Laboratory	Member
Ernest Rakaczky	Invensys Operations Management	Member
Alan Rivaldo	Public Utility Commission of Texas	Member
Julio Rodriguez	Idaho National Laboratory	Member
Mary Ann Roe	Elecsys Corporation	Member
David Sawin	Department of Transportation/Volpe Center	Member
Ryan Schnitzler	Lower Colorado River Authority	Member

Name	Organization	Role
Adam Schuerman	Dresden Nuclear Power Station	Member
Kenneth Shields	CPS Energy	Member
Walter Sikora	Industrial Defender, Inc.	Member
Brian Smith	EnerNex Corporation	Member
Darryl Song	Department of Transportation/Volpe Center	Member
Graham Speake	Yokogawa Electric Corporation	Member
Rich Stankevich	Owl Computing Technologies, Inc.	Member
Frances Staples	Department of Defense	Member
Clay Storey	Avista Corporation	Member
Michael Sweet	Energetics Incorporated	Member
Tatsuaki Takebe	Yokogawa Electric Corporation	Member
Scott Tampke	Elecsys Corporation	Member
Shawn Thomas	East Kentucky Power	Member
Mark Trump	FoxGuard Solutions	Member
Zachary Tudor	SRI	Member
Jeffrey Votion	CPS Energy	Member
Swapnil Wadikar	GE Energy	Member
Mark Wagner	Artemis Incorporated	Member
Cody Webb	Golden Spread Electric	Member
Robert Webb	ICS Secure, LLC.	Member
Mathew Weber	Salt River Project	Member
Charles Weissman	Los Angeles Metro	Member
Jack Whitsitt	Department of Homeland Security	Member
Scott Wise	US Navy	Member
John Wolf	Cliffs Natural Resources	Member
Timothy Yardley	University of Illinois	Member

CONTENTS

1. INTRODUCTION

Leaders from the nation's critical infrastructure sectors and government agencies recognize the need to plan, coordinate, and focus ongoing efforts to improve control system security. Industry stakeholders agree that a concise plan, with specific goals and milestones for implementing security across individual sectors, is required to prioritize critical needs and gaps to assist CIKR asset owners in reducing the risk of future cyber attacks on control systems.

In recent years, Energy, Water, Chemical, and other sector roadmaps have been developed to guide the efforts of individual sectors in securing their industrial control systems (ICSs). Roadmaps provide an opportunity for industry experts within a sector to offer their perspective concerning the state of control system cybersecurity and appropriate strategies for securing their sector. The Department of Homeland Security (DHS) is leveraging this industry perspective to coordinate the efforts across multiple CIKR sectors and help the sector stakeholder community develop programs and risk mitigation measures that align with the sector's plan while maintaining a cross sector perspective. In addition to the asset owners and operators, other sector stakeholders include industrial control system vendors, system integrators, and academia, which can use these roadmaps to map supporting activities with industry.

Because the roadmap goals are voluntary, implementation of the ideas and concepts presented in this document are addressed based on the organizations overall cybersecurity policies and procedures. Still, roadmaps are recognized as quality documents that provide excellent descriptions of industrial control systems risk challenges and general methods for improving the security of industrial control systems over the ensuing decade.

The specific challenges, goals, and priorities identified by the ICSJWG Roadmap Working Group are detailed in Section 3 of this roadmap.

ROADMAP PURPOSE

This roadmap builds on existing government and industry efforts to improve the security of industrial control systems within the private sector by working with sector-specific associations and agencies established to promote consistent application of standards and guidance within any given sector. Its intent is to help coordinate and guide related control system security efforts such as the International Society of Automation's (ISA) Committee on Industrial Automation Systems Security (ISA-99), National Institute of Standards and Technology (NIST), public and private research and development, and academic institutes supporting the development and promulgation of ICS security across multiple CIKR's. This roadmap:

- Presents a vision, along with a supporting framework of goals and milestones, to improve the cybersecurity posture of ICSs across all CIKR's
- Defines a consensus-based strategy that addresses the specific cybersecurity needs of owners and operators of CIKR facilities
- Proposes a comprehensive plan for improving the availability, security, reliability, and functionality of ICSs

Roadmap Purpose

- Define a consensus based strategy
- Propose a comprehensive plan to improve security
- Encourage stakeholder participation and compliance
- Guide industry, academia, and government effort
- Identify efforts for cross-sector cooperation
- Promote continuous improvement in security posture

- Proposes methods and programs that encourage participation and compliance by all stakeholders
- Guides efforts by industry, academia, and government
- Identifies opportunities for cooperative work across sectors
- Promotes continuous improvement in the security posture of ICSs within CIKR sectors, allowing sectors to establish baselines to measure security performance against established metrics. It should be understood that this is a living document which can and will change as the sectors mature in their security posture.

ROADMAP SCOPE

This roadmap addresses cybersecurity issues related specifically to ICSs owned and operated by agencies and industries whose facilities are part of the nation's CIKR's. The functional and organizational composition of CIKR sectors are defined in the National Infrastructure Protection Plan (NIPP)[1] and subordinate sector specific plans. Vendors that supply and maintain control systems components are an integral part of the cyber control system problem-solution space encompassed by this roadmap.[1]

Designing, operating, and maintaining a facility to meet essential availability, reliability, safety, and security needs as well as process control requirements requires the careful evaluation and analysis of all risk factors, including physical, cyber, and human. Attacks on a cyber system may involve only the cyber components and their operation, but those impacts can extend into the physical, business, human, and environmental systems to which they are connected. A cyber event, whether caused by an external adversary, an insider, or inadequate policies and procedures, can initiate a loss of system control, resulting in negative consequences. This roadmap recognizes this interconnectivity, but restricts its scope by addressing the cyber issues of ICSs.[2] Interactions with physical, business, and safety systems and their security components are an accepted reality necessitating the appropriate coordination of interfaces for secure and reliable operation.

Cyber risk to ICSs encompasses elements of the business network and Internet to the extent they are connected to process control systems. Securing access to and control of the business network and Internet is generally the responsibility of information technology (IT) personnel, and thus outside the scope of this roadmap. This roadmap does, however, include efforts to coordinate and interface with IT security efforts.

Physical access to cyber systems is a significant contributing factor of cyber risk. Similarly, physical damage resulting from cyber compromise is one of the principal factors contributing to industrial control systems risk. This roadmap includes both of these factors in understanding and planning for cybersecurity enhancements. However, actual engagement in physical access control and physical consequence management outside of physically securing cyber assets is beyond the scope of this roadmap.

This roadmap covers goals, milestones, and needs over the near (0–2 years), mid (2–5 years), and long (5-10 years) terms. Security needs encompass research and development (R&D), new technologies, systems testing, training and education, accepted industry practices, standards and protocols, policies, information sharing, and outreach and implementation.

[1] The sectors are bounded by the definition contained within the NIPP. The sector definitions within the NIPP result in companies and even facilities, that are in more than one sector

[2] This document uses the term "industrial control system" to include all process control systems, functional and operational systems, safety systems tied to operational systems, manufacturing execution systems, supervisory control and data acquisition systems (SCADA), and distributed control systems (DCS). It does not include business systems and strictly information systems.

NATIONAL CONTEXT

The Homeland Security Presidential Directive (HSPD)-7 *Critical Infrastructure Identification, Prioritization, and Protection* required NIPP to provide the collaborative framework and unifying structure for the integration of existing and future CIKR protection efforts for the government and private sector. These collaborative partnerships consist of a Sector Coordinating Council (SCC) and a Government Coordinating Council (GCC.)

HSPD-7 also assigned Sector-Specific Agencies (SSA's) for each of the 18 CIKR sectors, as the lead agencies responsible for collaborating with other Federal, State, local, tribal, territorial, and private sector partners. The SSA's, among other things, implement and encourage the development of information sharing and analysis mechanisms, including the sharing of information regarding physical and cyber threats, vulnerabilities, incidents, potential protective measures, and accepted industry practices. The NIPP requires sectors to issue sector-specific plans that address security posture and initiatives to achieve security.

SCCs are self-organized, self-run, and self-governed industry organizations that represent a spectrum of key stakeholders within a sector. SCCs serve as the government's principal point of entry into each sector for developing and coordinating a wide range of CIKR protection activities and issues.

In 2004, DHS NCSD established the Control Systems Security Program (CSSP), which was chartered to work with control systems security stakeholders through awareness and outreach programs that encourage and support coordinated control systems security enhancement efforts. In 2008, the CSSP also established the Industrial Control Systems Joint Working Group (ICSJWG) as a coordination body to facilitate the collaboration of control system stakeholders and to encourage the design, development and deployment of enhanced security for control systems.

Roadmap priorities and recommendations help inform and strengthen government programs designed to improve the protection of ICSs.

Appendix A summarizes national policy guidance on cybersecurity of industrial control systems.

ACTION PLAN

This roadmap proposes a strategic framework for addressing industrial control system security for both industry and government bodies. As an action plan, the roadmap is designed to improve resiliency against cyber events that would disrupt operations and have negative consequence to the nation's physical and economic security. Identified in this document are the challenges and activities that should be addressed and outlines specific milestones to be accomplished over the next 10 years to achieve the goals and vision outlined. While this plan contains many actionable items, it is only useful to the extent that financial resources, intellectual capability, commitment, and leadership translate these priorities and milestones into productive projects, activities, and products within their organizations.[3]

[3] See Section 6: References

2. CONTROL SYSTEM LANDSCAPE

ICSs perform various functions and exist at different stages of evolution throughout the nation’s CIKR. Many of the control systems used today were designed for availability and reliability during an era when security received low priority. These systems operated in fairly isolated environments and typically relied on proprietary software, hardware, and communications technologies. Infiltrating and compromising these systems often required specific knowledge of individual system architectures and physical access to system components.

In contrast, newer control systems are highly network-based and use common standards for communication protocols. Many controllers are Internet Protocol (IP) addressable. Asset owners and operators have gained immediate benefits by extending the connectivity of their control systems. They have increasingly adopted commercial off-the-shelf technologies that provide the greater levels of interoperability required among today’s modern infrastructures. Standard operating systems such as Windows, UNIX, or Linux are increasingly used in ICSs, which are now typically connected to remote controllers via private networks provided by telecommunications companies. Common telecommunications technologies such as the Internet, public-switched telephone, cable, or wireless networks are often used. A typical system configuration is shown in Figure 1.

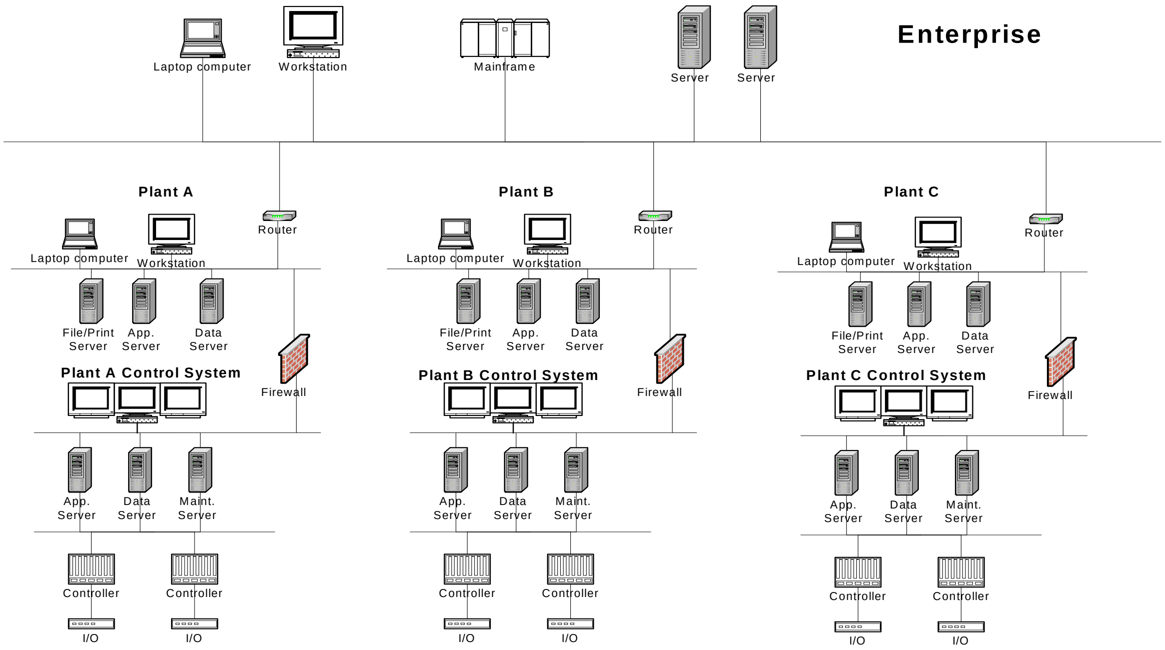


Figure 1. Components of a Typical Industrial Control System. (Source: ISA-99.00.01)

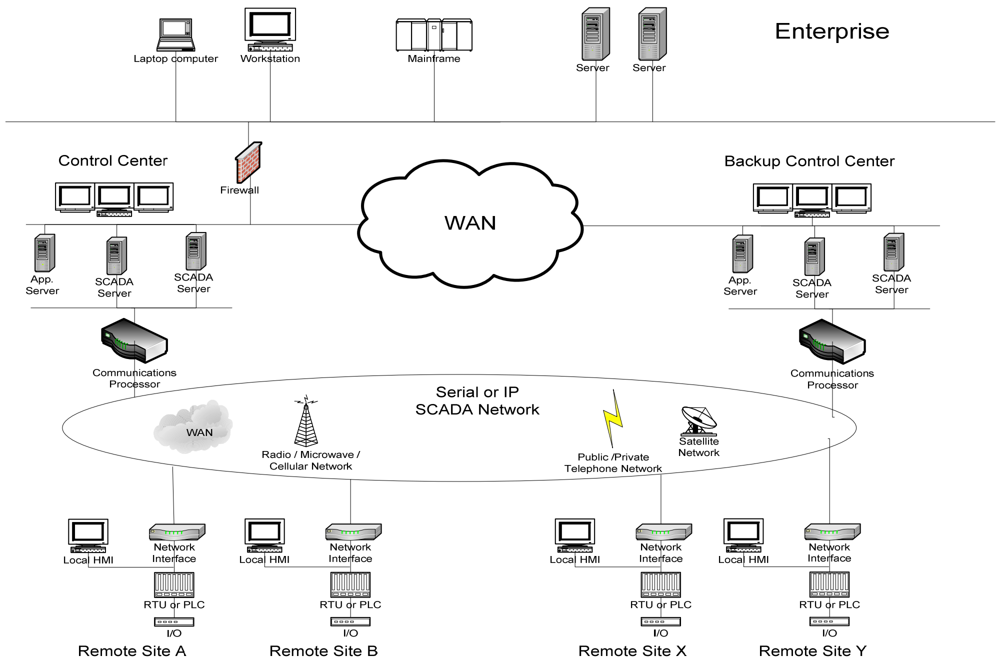
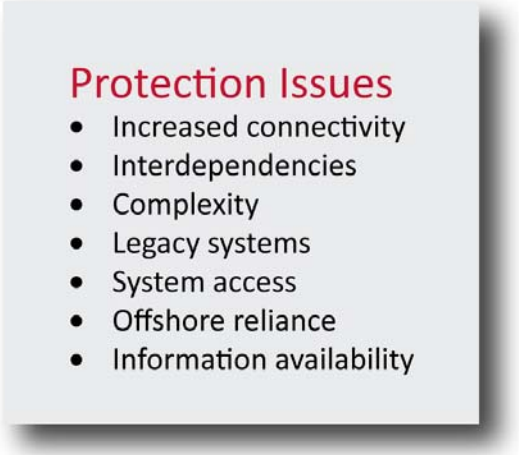


Figure 2. Components of a Typical SCADA System. (Source: ISA-99.00.01)



Protection Issues

- Increased connectivity
- Interdependencies
- Complexity
- Legacy systems
- System access
- Offshore reliance
- Information availability

The potential for system access resulting from this interoperability exposes network assets to infiltration and subsequent manipulation of sensitive operations. Furthermore, increasingly sophisticated cyber attack tools can exploit vulnerabilities in commercial off-the-shelf system components, telecommunication methods, and common operating systems found in modern control systems. The ability of asset owners to discover and understand such emerging threats and system vulnerabilities is a prerequisite to developing effective security polices and countermeasures.

Even though ICSs are designed for reliability (Availability, Integrity, Confidentiality), ICS security policies and practices are often poorly implemented. As operating practices have evolved to allow real-time operation and control of critical assets, protecting control systems from cyber risks has become more difficult. Some of the most serious security issues inherent in current industrial control systems include: increasing connectivity, proliferation of access points, escalating system complexity, greater interdependencies, increased outsourcing and reliance on foreign products, market restructuring, and wider use of common operating systems and platforms. These challenges contribute to the following heightened security risks in many CIKR sectors that employ industrial control systems:

- ***Increased Connectivity*.** Today's ICSs are being increasingly connected to company enterprise systems that rely on common operating platforms and are accessible through the Internet. Even though these changes improve operability, they also create serious vulnerabilities because improvements in the security features of control systems are not concurrent.
- ***Interdependencies.*** Due to the high degree of interdependency among infrastructure sectors, failures within one sector can spread into others. A successful cyber attack might be able to take advantage of these interdependencies to produce cascading impacts and amplify the overall economic damage.
- ***Complexity.*** The demand for real-time information-sharing and control has increased system complexity in several ways: access to ICSs is being granted to more users, business and control systems are interconnected, and the degree of interdependency among infrastructures has increased. Dramatic differences in the training and concerns of those in charge of IT systems and those responsible for control system operations have led to challenges in coordinating network security between these two key groups.
- ***Legacy Systems.*** Although older legacy ICSs may operate in more independent modes, they tend to have inadequate password policies and security administration, no data protection mechanisms, and protocols that are prone to snooping, interruption, and interception. These insecure legacy systems have long service lives and will remain vulnerable for years to come unless these problems are mitigated.
- ***System Access.*** Even limited connection to the Internet exposes control systems to all of the inherent vulnerabilities of interconnected computer networks, including viruses, worms, hackers, and terrorists. Control channels that use wireless or leased lines that pass through commercial telecommunications facilities may also provide minimal protection against forgery of data or control messages. These issues are of particular concern in industries that rely on interconnected enterprise and control networks with remote access from within or outside the company.
- ***Offshore Reliance.*** Many software, hardware, and control system manufacturers are under foreign ownership or develop systems in countries whose interests do not always align with those of the United States. Also of concern is the practice of contracting control systems' support, service, and maintenance to third parties located in foreign countries.
- ***Information Availability.*** Manuals and training videos on control systems are publicly available and many hacker tools can now be downloaded from the Internet and applied with limited system knowledge. Attackers do not have to be experts in control operations.

A more in-depth description of typical ICSs and their vulnerabilities and currently available general security enhancements can be found on the United States Computer Emergency Readiness Team (US-CERT) Control System website at http://www.us-cert.gov/control_systems/csvuls.html, and the soon to be completed National Institute of Standards and Technology Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security, Recommendations of the National Institute of Standards and Technology."[4]

[4] See Section 6: References

A FRAMEWORK FOR SECURING CONTROL SYSTEMS

Protecting industrial control systems is a formidable challenge requiring a comprehensive approach that addresses the urgent security concerns of today's systems while preparing for the needs of tomorrow. Asset owners and operators must understand and manage cyber risks, secure their legacy systems, apply security tools and practices, and consider new control system architectures—all within a competitive business environment. Government has a large stake in the process because infrastructure sectors are critical to national security and have interdependencies that could result in cascading impacts during a cyber attack or event. Still, cybersecurity enhancements must compete with other investment priorities, and many executives find it difficult to justify security expenditures without a strong business case. Sector specific roadmaps play an essential role in supporting the national strategy to articulate the essential goals for improving control system security and to align and integrate the efforts of industry and government to achieve those goals.

This roadmap is structured around a framework of establishing a vision, defining top-level goals aimed at achieving that vision, and then identifying the challenges associated with the goals. Actions are then identified that, if implemented and successful, will address the challenges and assist in meeting the goals; a key set of these actions are identified as priorities. Finally, a set of milestones are selected from within the priorities and tied to dates so that progress towards achieving the goals can be monitored and measured.

The various individual CIKR sectors control systems in total constitute a larger system of systems. Although they operate independently, their interdependencies typically express important emergent properties and critical dependencies. The system of systems approach incorporates the interactions of technology, policy, and economics in a general process including design, complexity and systems engineering, and modeling. These systems of systems typically exhibit the behaviors of complex systems with combinations of traits such as:

- Operational Independence of Elements
- Managerial Independence of Elements
- Evolutionary Development
- Emergent Behavior
- Geographical Distribution of Elements
- Inter-disciplinary Study
- Heterogeneity of Systems
- Networks of Systems

The first five traits are known as Maier's criteria for identifying system of systems challenges. The remaining three traits have been proposed from the study of mathematical implications of modeling and analyzing system of systems challenges.

This CIKR sector system of systems is very similar to the concept of a sustainable community where each individual system is optimized in relation to the entire community system, resulting in increased robustness, survivability, and resiliency. A similar concept is potentially applicable to the securing of control systems within the CIKR sector system of systems.

VISION

The vision of the ICSJWG Roadmap Working Group is:

> *Within 10 years, control systems throughout the CIKR sectors and Federal Partners will be able to operate securely, robustly, and resiliently; and be protected at a level commensurate with risk. Control systems throughout the CIKR sectors and Federal Partners will be able to operate with no loss of critical function in vital applications during and after a cyber event without impacting the overall mission of the facility.*

This roadmap is envisioned to serve as an initial framework and mechanism to provide asset owners/operators, vendors, and the Federal government with goals, recommendations, and guidelines focused on enhancing control systems security to a level at which each Sector is able to mitigate cybersecurity problems in a cost effective manner relative to the risk.

CONTROL SYSTEMS SECURITY GOALS

Today's ICSs have become an essential element in the management of complex processes and production environments. The risk of exploitation by physical or cyber means with the intent to cause harm is real and can have negative impacts on an asset owner's business, public safety, the environment, and national security. Asset owners within the nation's CIKR must understand and manage this risk by securing their installed systems, conducting vulnerability assessments, applying security tools and practices, and considering security as they procure and install next-generation systems. Even though the majority of CIKR assets are owned and operated by private industry or local governments, the Federal government has a large stake in this effort because the consequences of these risks could have negative impacts on society and national security.

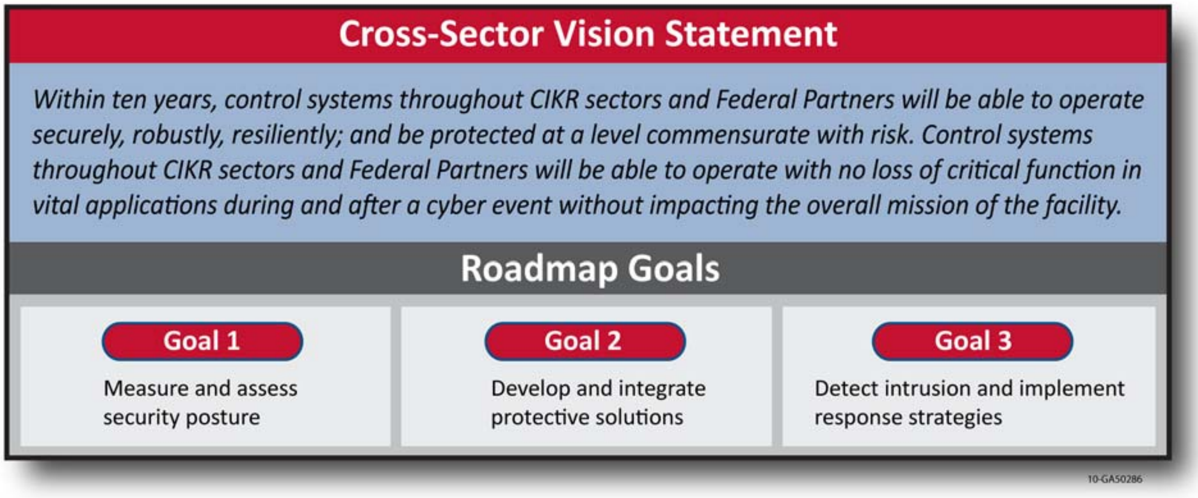
Attention to ICSs cybersecurity has been increasing over the past several years. Therefore, based on this raising of awareness and lessons learned in the development of other sector roadmaps, three goals have been selected as the guiding objectives of this roadmap. These goals are structured after rather classical security models that measure and assess, protect, detect, defend (detain or eliminate as may be required), recover, build-in security (rather than attaching it as an after-thought), and provide continual improvement. These goals encompass technical, programmatic, management, and cultural achievements, and help to facilitate a partnership between asset owners, ICSs vendors, and regulators to make security an integral part of the specified and produced systems. The following list briefly describes each goal:

Measure and assess security posture. Implied in the successful use of any roadmap is knowing where you are, or in the case of the ICSJWG Roadmap, knowing the current state of your security posture. Therefore, as part of the ICSJWG Roadmap, a tool and methodology are provided in order to give this capability to every sector that employs industrial control systems.

Develop and integrate protective measures. As security problems are identified or anticipated, protective measures will be developed and applied to reduce system vulnerabilities, system threats, and their consequences. Appropriate security solutions will be devised by the sector, as well as vendors and R&D organizations outside the sector. However, the application of security solutions to legacy systems will be constrained by the inherent limitations of existing equipment and configurations. As legacy systems age, they will be replaced or upgraded with next-generation control system components and architectures that offer built-in, end-to-end security. This replacement will typically not be driven solely by security-related concerns. A practical goal is to encourage R&D into tying legacy systems into upcoming security solutions.

Detect intrusion and implement response strategies. Cyber intrusion tools are becoming sophisticated to the degree that any system vulnerability can become exposed to emerging threats. More effective and sophisticated exploits are more common now with less sophisticated adversaries launching them (e.g., script kiddies, rootkits, etc.) Within 10 years, CIKR Sectors will be operating networks that automatically provide contingency and remedial actions in response to attempted intrusions.

Maintaining aggressive and proactive cybersecurity of ICSs over the long term will require a strong and enduring commitment of resources, clear incentives, and close collaboration among stakeholders. Over the next 10-years, CIKR Sector owners and operators will collaborate within the sector, across sectors, and with government to remove barriers to progress and create policies that accelerate a sustained advancement in securing their ICSs by continuously reiterating on the above three goals.[4]



Cross-Sector Vision Statement

Within ten years, control systems throughout CIKR sectors and Federal Partners will be able to operate securely, robustly, resiliently; and be protected at a level commensurate with risk. Control systems throughout CIKR sectors and Federal Partners will be able to operate with no loss of critical function in vital applications during and after a cyber event without impacting the overall mission of the facility.

Roadmap Goals

Goal 1	Goal 2	Goal 3
Measure and assess security posture	Develop and integrate protective solutions	Detect intrusion and implement response strategies

3. CHALLENGES AND MILESTONES

This section addresses the challenges facing control system security, the priorities that need to be addressed, and the goals selected to guide the efforts to improve the cybersecurity posture of individual asset owners. It also describes the selected milestones established to support the implementation of the goals.

CHALLENGES FOR SECURING CONTROL SYSTEMS

Challenges to cybersecurity consist not only of the direct risk factors that increase the probability of a successful attack and the severity of the consequences but also of those factors that limit the ability to implement ideal security enhancements.

Risk Challenges to Cyber Security

- Threat
- Means of attack
- Nature of the system attacked
- Value of material and systems attacked
- Interaction caused by loss of control

Risk is defined as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. The three components of risk are:

- threat - defined as a natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property;
- vulnerability - which is a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard; and
- consequences - also known as the effect of an event, incident, or occurrence.
    - Evaluating consequences: The consequences of a cyber attack may involve impacts to confidentiality, integrity, or availability (CIA) of a control system or its data:
        - Confidentiality impacts involve the unauthorized disclosure of information. This might involve sensitive information such as descriptions or data of control system operations, facility processes, or system security.
        - Integrity impacts involve the loss of control over system operation or the data being used by the control system. A loss of integrity can involve the unauthorized modification, insertion, or destruction of data or controlling software.
        - Availability impacts involve the ability of a control system to perform its function as needed. Loss of availability can arise from a denial or disruption of communications or inability of the control system to perform its designed function.

The direct risk challenges include:

- the threat (those who seek to attack and compromise cyber system);
- the means of attack (which relies on taking advantage of system vulnerabilities);

- the nature of the system attacked (such as the age and configuration of the system);
- the value of the systems; and
- how loss of control impacts the interaction with humans, property, and the environment.

Challenges related to the implementation of security enhancements include organizational, institutional, economic, and technical factors that either limit the availability of security solutions, or increase the difficulty of implementing the optimum security enhancements. Many of these security challenges have been discussed and tabulated over the past 10 years. An example would be getting wholesale, self-motivated buy-in by the people within utilities charged with cybersecurity and encouraging/motivating companies in the sector to include implementation of cybersecurity solutions and reaching the goals in the roadmaps as part of performance reviews of the designated humans involved.

MILESTONES FOR SECURING CONTROL SYSTEMS

The challenges in securing control systems are minimized or overcome through the achievment of security milestones. Often these milestones begin as a simple reversal of the challenge. For example, Challenges—lack of knowledge, limited standards, limited capabilities, and need for a business case—lead to milestones of enhancing training, improving standards, and enhancing capabilities, and the development and use of risk analysis, respectively. A brief summary of milestone development followed by a graphical depiction of the challenges and milestones for each goal are presented below.

An important part of the performance management process used to meet milestones is the setting and evaluation of SMART objectives. They are the link to overall performance and provide clear and precise measures of what is required of participants and by when. Performance objectives should relate directly to overall priorities and objectives to ensure that efforts are focused on helping the overall program meets its targets.

SMART means:

Specific	Describes an observable action or the end state which can be seen when the performance objective has been achieved. In other words, what specifically is to be accomplished?
Measurable	Quantifiable criteria for evaluating the accomplishment of the objective. In other words, how much? Determine the methods, timing and tools used to arrive at the measurement.
Achievable	Describes a result that can be realistically achieved even though the objective may be challenging.
Relevant	Directly aligned to the program priorities and objectives.
Time-bound	Indicates the time schedule or deadline for achieving the performance objective. In other words, by when?

CHALLENGES AND MILESTONES FOR GOAL 1: MEASURE AND ASSESS SECURITY POSTURE

Goal 1 suggests that each participating CIKR execute a methodology such as the one outlined in Section 4: Sector Cybersecurity Posture. Although there are many methodologies, training programs, standards, and accepted industry practices to understand and measure risk (comprised of vulnerabilities, consequences, and threats) and other technical factors that could contribute to a composite measurement of cybersecurity posture, the ICSJWG Roadmap has taken a more high-level programmatic approach to determining cybersecurity posture. The ICSJWG Roadmap represents the consensus of those who have contributed to its making as one method to holistically and effectively measure cybersecurity posture.

While the ICSJWG Roadmap outlines a means to overcome some of the current challenges to the precise quantification of cybersecurity postures, there is clear recognition that these challenges won't go away and must be addressed. There is general agreement that while many challenges remain, the CIKR Sector and hence the Nation are best served by providing even a high-level assessment today as we transition to a more mature and quantifiable process tomorrow.

Currently, asset owners and operators can have difficulty obtaining necessary inventories of their critical assets and associated ICSs. Also, an understanding of the risk (threats, vulnerabilities and consequences) of a cyber attack is often inadequate. The growing number of nodes and access points has made identifying vulnerabilities more complex. Many industry practices exist for ICS risk measurement, metrics, and measuring tools do exist and are reflected by many standards, metrics, and specifications across the sector, but there is no industry consensus on even the most basic notion of how to measure cybersecurity. However, tools, methods and standards for measuring security are essential to assessing the security/risk of these increasingly complex control systems and all of their components and links.

CHALLENGES:

Understanding Risk

- Inventory of critical assets, their associated ICSs, and the risk of cyberattacks are often not adequately known or understood
- Knowledge and understanding of risk, including threat, vulnerability, defense, and consequence analysis capabilities across CIKR sectors are limited
- Cybersecurity risk factors are neither widely understood nor commonly accepted by technologists and managers
- Security vulnerability assessments (SVA), ideally supplemented with an external SVA, are needed to determine the consequences of specific cybersecurity compromises of ICSs
  - The DHS developed Cybersecurity Evaluation Tool (CSET) provides one way for users to perform a security vulnerability assessment
- Developing a Sector-Wide understanding of the cybersecurity posture

Physical Issues

- Physical and electronic isolation (air gap) of many facilities may provide a false sense of security from a broad range of advance persistent threats

Measuring Risk – Metrics, Standards, Quantifications

- Cybersecurity threats are difficult if not impossible to quantify, but quantified values are required for quantified risk estimation. Sometimes only a qualitative understanding of threat is available and hence, only an impact style evaluation can be developed. In these cases the development of the consequences and vulnerabilities are needed.
- Current standards for assessment of cyber vulnerabilities must be chosen carefully
- Many existing standards lack meaningful and measurable specification relating to ICSs cybersecurity
- Consistent metrics are necessary but not always readily available to measure and assess cybersecurity status
- Metrics to quantify cybersecurity and/or improvements over time and across the sector are needed but not available

MILESTONES:

Near-Term

There are two components to the first near-term milestone. The first component will focus on the deployment and adoption of the Cybersecurity Posture Assessment tool which includes the use of the Cybersecurity Evaluation Tool (CSET) for ICS security vulnerability assessments.

The second component (on a parallel track) will focus on the establishment of common metrics for benchmarking ICSs risk through CIKR Sectors; the integration of security into operation plans; and the dissemination of accepted ICSs standards and guidelines that enable the tools and metrics to be effectively deployed.

Mid-Term

Mid-term milestones involve the implementation and use of automated assessment tools in ICSs and the development of real-time security assessment capabilities for new and legacy systems. These milestones also involve sector-wide dissemination of training programs and recommended guidelines, in conjunction with the CSET which will continue to assist and improve capabilities of asset owners and operators in performing cybersecurity self-assessments against cybersecurity vulnerabilities. However, most facilities still require guidance and support to use these tools.

Long-Term

The long-term milestone associated with this goal helps to institutionalize the practice of ICSs risk assessment with the development and implementation of fully automated security state monitors and response systems in most ICSs networks, and the practice of actively measuring performance and benchmarking with other sectors.

GCC and SCC can develop more specific and accurate understandings of the Sector's security posture and reflect this in the annual update to the SSP.

Due Date:

Near Term (0-2 years)

- Adopt and use the Cybersecurity Posture Assessment tool
- Integration of security into all operational plans
- Development of common risk assessment metrics and standards
- Development of automated tools to assess cybersecurity and compliance with pertinent regulations
- Implementation of risk assessment tools throughout the CIKR Sectors as asset owners and operators begin performing self-assessments

Mid Term (2-5 years)

- Implementation of training programs throughout the CIKR Sectors on the control system security recommended guidelines
- Integration of control system security education, awareness, and outreach programs into CIKR Sector operations
- Implementation of standardized or consistent risk assessment tools throughout the CIKR Sectors

Long Term (5-10 years)

- Development of fully automated security state monitors in most control systems networks
- Industry-wide active assessment of ICS security profiles including benchmarks against other sectors

CHALLENGES AND MILESTONES FOR GOAL 2: DEVELOP AND INTEGRATE PROTECTIVE SOLUTIONS

Goal 2 calls for actionable efforts, when security vulnerabilities are identified and security postures assessed, to implement and apply protective solutions as well as developing new solutions to reduce system vulnerabilities, system threats, and their consequences.

Periodic nondestructive testing of control systems should be implemented to verify that the systems, as designed, installed, and maintained, are effective in detecting, isolating, and automatically responding to cyber attacks.

For legacy systems, protective solutions often include the application of proven best practices and security tools, procedures and patches for fixing known security flaws, training programs for staff at all levels, and retrofit security technologies that do not degrade system performance. As these legacy systems age, they will be replaced or upgraded with next-generation control system components and architectures that offer built-in end-to-end security.

Many ICSs have poorly designed connections between control systems and enterprise networks, use unauthenticated command and control data, and do not use adequate access control for remote access points. For example, the widespread use of wireless communication and remote access has opened up additional vulnerabilities that need to be mitigated with secure and cost efficient systems and components. In some cases, access control capability is available for ICSs, however, it may not have been enabled or implemented properly (e.g., by using the default vendor passwords or allowing sharing of passwords). In addition, security improvements for legacy systems are limited by the existing equipment and architectures that may not be able to accept security upgrades without degrading performance, which indicates that R&D should be encouraged to do more to improve the access control security of legacy systems.

CHALLENGES

Access Issues (open environments, remote access, multiple access points)

- Widespread and continuous connectivity of IT and ICSs, and generally, with remote access by multiple parties or devices
- Many ICSs have remote access points without appropriate or adequate access control
- Many ICSs have been designed, built, and operated within open communication environments
- Existing ICSs have numerous access points, use default vendor accounts/passwords/ shared passwords, and have poor firewall implementation
- Many ICSs operate using unauthenticated command and control data
- Basic security features are often not enabled on ICSs
- The complexity of ICSs increases exponentially with an increase in the number of nodes.
- The use of COTS greatly increases the risk of an ICSs

Legacy Upgrade and Patch Management Issues

- The unavailability of patch management that conforms to a 24/7 operating environment with extended vulnerability windows and without regularly scheduled maintenance opportunities
- Older operating platform (legacy and hybrid) systems may have limited or no vendor support, thus limiting their ability to secure the system
- Security upgrades are hard to retrofit to legacy ICSs, may be costly, and may degrade system performance, thus lessening incentives to upgrade those systems

MILESTONES

Near-Term

Near-term milestones for this goal involve the development of control system protection guidelines that assist in ensuring existing access controls are properly implemented and enabled. These guidelines should be disseminated widely throughout all CIKR Sectors, along with additional training materials regarding cyber and physical security for control systems. Also during this time, mechanisms should be established for sharing information between asset owners and operators and vendors to develop improved protection tools. Lastly, security patches for common vulnerabilities should be developed, implemented and widely distributed among asset owners and operators.

Mid-Term

Mid-term milestones focus on the implementation of new protective tools as well as securing the interfaces between ICSs and business systems. This includes securing connections between remote access points and control centers. The milestones also call for training programs to support proper use and protocol for these new tools and systems. Training courses for asset owners and operators should continuously be developed and updated to help increase awareness and facilitate culture shifts in ICSs security practices. Ideally, there should be a forum within the ICSJWG putting asset owners and vendors together to describe what's needed based on the recommended practices and what's possible in the short and long term regarding actual solutions.

Because the application of control systems varies across sectors, the sector should identify, publish, and disseminate recommended practices regarding control system security. These recommendations should cover such diverse topics as securing connectivity with business networks and for providing physical and cybersecurity for remote facilities.

Long-Term

The long-term milestone for Goal 2 focuses on securing the integration of ICSs to any external system as well as the installation of cyber resilient ICSs architectures that have built-in security and use systems and components that are secure-by-design.

Due Date:

Near Term (0-2 years)

- Development of control system protection guidelines for existing ICSs
- Development and implementation of security patches for legacy systems
- Establishment of mechanisms to enhance information sharing between asset owners and operators and vendors
- Development of guidance and education material associated with applicable project regulations
- Development of guidelines to secure or isolate ICSs communications from public networks and communication infrastructures

Mid Term (2-5 years)

- Implementation of new protective tools and appropriate training
- Implementation of secure interfaces between ICSs and business systems

- Identification, publication, and dissemination of recommended practices, including ones for securing connectivity with business networks and for providing physical and cybersecurity for remote facilities
- Development of high-performance, secure communications for legacy systems

Long Term (5-10 years)

- Secure integration of ICSs and business systems

CHALLENGES AND MILESTONES FOR GOAL 3: DETECT INTRUSION AND IMPLEMENT RESPONSE STRATEGIES

Cyber intrusion tools are becoming increasingly sophisticated such that protection of ICSs from all cyber threats is not possible. Goal 3 focuses on the sector's resilience in the face of a successful attack. Resilience suggests that facilities have the ability to monitor system integrity and detect intrusions with sophisticated alarming tools. This goal also suggests the capacity to analyze anomalies and manage security events and response strategies. Finally, it suggests automated incident reporting processes that include complete audit trails. Ideally, CIKR Sectors are envisioned to be operating networks that automatically provide contingency and remedial actions in response to attempted intrusions.

Due to concerns regarding proprietary information, asset owners and operators often do not share information beyond the company regarding past security events and their consequences. In addition, companies may not regularly review security logs. The failure to review and share lessons learned limits response capability in an emergency, even when appropriate security measures are available.

Another major challenge to implementing response strategies is that some measures taken to increase ICSs protection may inhibit the capacity to implement quick response strategies in emergencies. For example, in an emergency an operator may need to access control programs in order to mitigate damages and bring the system back on. However, increased access controls could prevent the person most able to fix the system from logging in.

CHALLENGES

- Periodic and appropriate reviews of security logs and change management documentation often receive limited, if any, attention
- Cybersecurity protection measures can negatively impact ability to rapidly respond to emergencies
- It is difficult to keep up with the continuous increase in the sophistication and availability of hacker's tools and resources

MILESTONES

Goal 3 suggests provisions to detect and respond to the attacks that manage to defeat the protective solutions of Goal 2.The milestones for Goal 3 are therefore directed towards ICSs incident handling, including detection, response, and recovery from an all-hazards perspective.

Near-Term

In the near-term, security features already built into control systems should be identified and enabled as appropriate. Cyber incident response and recovery plans should be developed and incorporated into well-established emergency operating plans. CIKR Sector members should also focus on identifying recommended practices and approved guidelines for incident reporting as well as improved methods for information sharing. In the near term, asset owners and operators should also be engaging employees in proper training on incident response procedures and begin working with vendors on specifications for new detection and response tools for ICSs systems.

Mid-Term

By the mid-term, new and improved detection, response and recovery tools with greater effectiveness should be developed and implemented. Examples include: intrusion detection systems that perform complete audit trails and automated reporting; tools that help visualize data and communication patterns for identifying anomalies and correlate suspicious patterns with potential threats; and tools for security event management which helps prioritize corrective actions through alarming, trending, forensics, and audits.

In addition, emergency response plans and training procedures should be updated to reflect changes in new tools and recommended practices. Employee training programs should be conducted to ensure correct implementation of new ICSs tools and procedures. Assets owners and operators may also want to develop public communication strategies such as providing public safety training literature on consequences of a disruption from a cyber event.

Long-Term

Widespread implementation and use of automated self-healing control system architectures is a major long-term milestone. Within ten years, ICSs detection and response tools should have the capability of performing real-time detection and response and should develop control system security certification programs for operators.

Due Date:

Near Term (0-2 years)

- Leverage development of accepted industry practices on control system architecture and protection
- Integration of cyber incident response plan and procedures into emergency plans
- Identification and implementation of current security features built in the control system
- Development of recommended practices and guidelines for incident reporting
- Development of partnerships between asset owner/operators and vendors to develop intrusion detection software for sector use
- Timely dissemination of control system risk information to CIKR Sector community

Mid Term (2-5 years)

- Implementation of intrusion detection software in monitoring sector ICSs, publication of related recommended practices and guidelines and provision of related training
- Implementation of training programs for new intrusion detection software and any associated updates to response, identification and reporting procedures
- Development of control systems simulators to perform the operator training
- Development of training for control room operators in identifying and reporting unusual events, breaches, and anomalies from a cyber event
- Implement configuration management procedures and test beds for patch installations
- Development of public communication strategies and dissemination of public safety training literature on consequences of a disruption from a cyber event

Long Term (5-10 years)

- Development and installation of self-healing control system architecture throughout the CIKR Sectors
- Implementation of real-time intrusion detection and prevention systems
- Development of control systems security certification program for operators

4. SECTOR CYBERSECURITY POSTURE

As previously stated, one of the purposes of creating a cross-sector roadmap is to find the common denominators and drive improvements across all CIKR Sectors. In other words, each sector's SSP will address sector specific issues, challenges and solutions that are unique to each sector, but the ICSJWG Roadmap will identify those things that all sectors could be doing to improve their cybersecurity posture over time.

Most of the activities described herein are being performed by the CIKR Sectors to some degree in cooperation with existing DHS programs within the NCSD, other organizations such as the MS-ISAC, and through various standards development organizations like NIST, ISA, IEC, and IEEE. The ICSJWG Roadmap will fully capitalize on those existing programs and thus tie together multiple efforts. This methodology provides a means to gauge Roadmap implementation and hence provide a view into the cybersecurity posture of all CIKR's that use and depend on ICSs.

The ICSJWG has outlined a suggested set of performance metrics that can be aggregated at the sector level to represent all CIKR's that use control systems and illustrate the progress that is being made toward a more secure and robust national infrastructure. By necessity, any tool or process capable of looking at ICSs cybersecurity across all sectors must be at a relatively high level. To that end, this Section will outline:

- A notional cybersecurity posture assessment tool
- The performance metrics used to measure current status
- A means to show progress on the performance metrics over time

Metrics can be used for self evaluation, situational awareness, and performance determination. The intent of this section is to establish a methodology that can be used to evaluate security posture throughout operating, budgetary or capital modification cycles.

Monitoring and improving a Sector's cybersecurity posture will continue to be an ongoing and challenging effort. As ICSs continue to become more Internet dependent, an increasing need for quantifiable metrics for determining progress and performance on measures of cybersecurity exists. As such, the Roadmap ICSJWG has attempted to develop a methodology pursuant to what can be done today to improve the situation knowing that cybersecurity is a moving target, but many of the existing programs and standards have been designed through a consensus process to reflect the collective wisdom of the ICS industry. In other words, the ICSJWG Roadmap makes recommendations recognizing that cybersecurity is a never-ending endeavor.

ICSs CYBERSECURITY POSTURE METRICS

One way to represent cybersecurity posture uses seven specific areas of performance and establishes a score associated with each of the seven performance areas. The following seven performance areas can be used to measure the relative cybersecurity posture of a given CIKR Sector, but they can also be aggregated across multiple Sectors.

1. Security Vulnerability Assessment (e.g., CSET Tool Usage)
2. Information Sharing
3. Certifications and Accreditations
4. Procurement Language

5. Security Awareness Training
6. Standards
7. Incident Response Planning

The process for determining a baseline performance score is achieved in two parts. First, using Table 5.1, identify current assessment level scores (1 - 5) associated with each of the seven performance areas. Second, plot the scores on the Security Posture Assessment Graph, Figure 5.1. The scoring for each performance area improves as the number decreases. The overall numerical score as well as the plotted graphic can be used to establish and visually perceive potential vulnerabilities and weaknesses in initial/baseline cybersecurity postures or indicate overall programmatic imbalances.

Each individual CIKR Sector that implements the ICSJWG Roadmap and adheres to its tenets should progress toward a lower overall numerical score as well as achieving more symmetry within the graph. Symmetry would indicate a programmatic balance in all areas that can affect the cybersecurity posture.

Although the metrics and performance measures provided herein provide an indicator of the overall CIKR Sector cybersecurity posture, this is also their limitation. In other words, they are high-level indicators of the actual security posture rather than absolute measurements and should not be imbued with any weight beyond that.

Table 1. Performance Measurement Determination

ICSs Cybersecurity Metrics and Performance Measures

Score	5	4	3	2	1
1.0 Security Vulnerability Assessments (SVA)	Evidence exists that less than 25% of the 18 CIKR's are performing an SVA (e.g., CSET)	Evidence exists that nominally 25% of the 18 CIKR's are performing an SVA (e.g., CSET)	Evidence exists that nominally 50% of the 18 CIKR's are performing an SVA (e.g., CSET)	Evidence exists that nominally 75% of the 18 CIKR's are performing an SVA (e.g., CSET)	Evidence exists that nominally 100% of the 18 CIKR's are performing an SVA (e.g., CSET)
2.0 Information Sharing	Evidence exists that less than 25% of the 18 CIKR's are connected to the relevant ISACS, CERTs, or other means	Evidence exists that nominally 25% of the 18 CIKR's are connected to the relevant ISACS, CERTs, or other means	Evidence exists that nominally 50% of the 18 CIKR's are connected to the relevant ISACS, CERTs, or other means	Evidence exists that nominally 75% of the 18 CIKR's are connected to the relevant ISACS, CERTs, or other means	Evidence exists that nominally 100% of the 18 CIKR's are connected to the relevant ISACS, CERTs, or other means
3.0 Certifications and Accreditations	Evidence exists that less than 25% of the 18 CIKR's have employed certified professionals or accredited systems	Evidence exists that nominally 25% of the 18 CIKR's have employed certified professionals or accredited systems	Evidence exists that nominally 50% of the 18 CIKR's have employed certified professionals or accredited systems	Evidence exists that nominally 75% of the 18 CIKR's have employed certified professionals or accredited systems	Evidence exists that nominally 100% of the 18 CIKR's have employed certified professionals or accredited systems

ICSs Cybersecurity Metrics and Performance Measures

Score	5	4	3	2	1
4.0 Procurement Language	Evidence exists that less than 25% of the CIKR's have implemented the standard Procurement Language in their acquisitions for control systems	Evidence exists that nominally 25% of the CIKR's have implemented the standard Procurement Language in their acquisitions for control systems	Evidence exists that nominally 50% of the CIKR's have implemented the standard Procurement Language in their acquisitions for control systems	Evidence exists that nominally 75% of the CIKR's have implemented the standard Procurement Language in their acquisitions for control systems	Evidence exists that nominally 100% of the CIKR's have implemented the standard Procurement Language in their acquisitions for control systems
5.0 Security Awareness Training	Evidence exists that less than 25% of the CIKR's have implemented mandatory security awareness training	Evidence exists that nominally 25% of the CIKR's have implemented mandatory security awareness training	Evidence exists that nominally 50% of the CIKR's have implemented mandatory security awareness training	Evidence exists that nominally 75% of the CIKR's have implemented mandatory security awareness training	Evidence exists that nominally 100% of the CIKR's have implemented mandatory security awareness training
6.0 Standards	Evidence exists that less than 25% of the CIKR's have implemented security standards such as NIST, ISA, IEEE, IEC	Evidence exists that nominally 25% of the CIKR's have implemented security standards such as NIST, ISA, IEEE, IEC	Evidence exists that nominally 50% of the CIKR's have implemented security standards such as NIST, ISA, IEEE, IEC	Evidence exists that nominally 75% of the CIKR's have implemented security standards such as NIST, ISA, IEEE, IEC	Evidence exists that nominally 100% of the CIKR's have implemented security standards such as NIST, ISA, IEEE, IEC
7.0 Incident Response Planning	Evidence exists that less than 25% of the CIKR's have implemented any incident response planning	Evidence exists that nominally 25% of the CIKR's have implemented any incident response planning	Evidence exists that nominally 50% of the CIKR's have implemented any incident response planning	Evidence exists that nominally 75% of the CIKR's have implemented any incident response planning	Evidence exists that nominally 100% of the CIKR's have implemented any incident response planning

ICSs Security Posture Within a Given CIKR

A graphical representation of the self-assessment is used to make relative comparisons within a single sector from year to year or comparisons between sectors. However, as these measures are not adjusted or weighted (because some measures may be irrelevant for a given sector) the best use is to show relative improvement over time for a given sector or aggregated to show progress over time for the entire ICSs industry.

The benefit of this graphical representation is that overlays from previous performance periods can be overlaid to show progress or maturity throughout the seven performance areas. The overall intent of each sector should be to progress, over time, toward a lower numerical score, while maintain an appropriate level of symmetry in the graph indicating programmatic balance and a maturing cybersecurity posture.

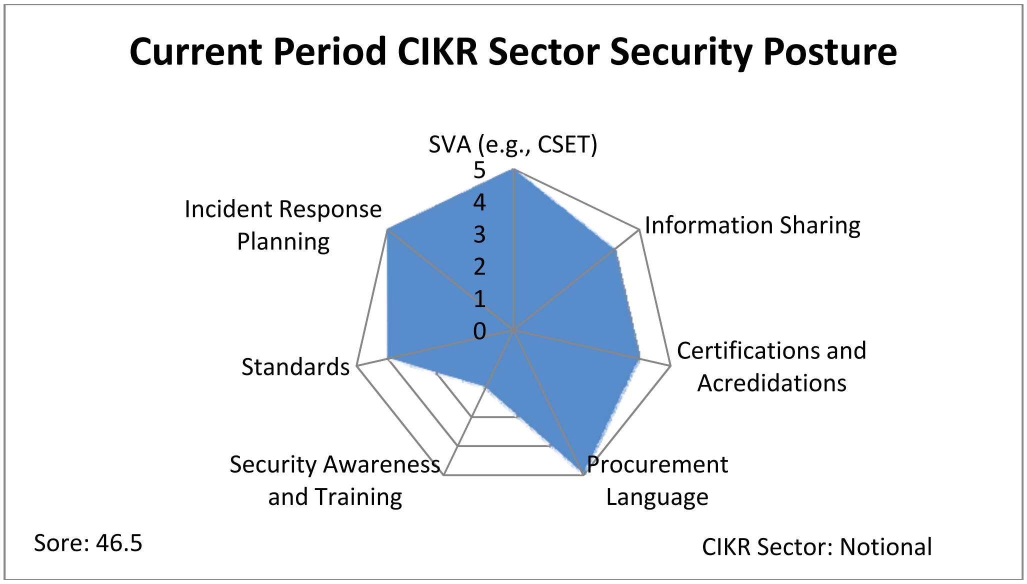


Figure 3. Security Posture Assessment Graph

CROSS-SECTOR ICSS CYBERSECURITY POSTURE

On a quarterly, annual or other periodic cycle, the individual CIKR sector measurements can be aggregated to present a view of ICSs cybersecurity posture and can be tracked over time to indicate progress toward more robust and secure ICSs. As performance is tracked/trended in each of the seven areas or collectively, the results can be presented in graphical form, as shown in Figure 5.2.

The objective of each sector should be toward improving their cybersecurity posture throughout their ICS networks. These metrics and graphics allow for a snapshot of current cybersecurity postures. As cybersecurity matures within a sector, these graphics can provide evidence for such improvements and progress. This ICSJWG Roadmap will likewise mature and evolve as a living document, establishing additional areas for improvement and methods of implementation over time.

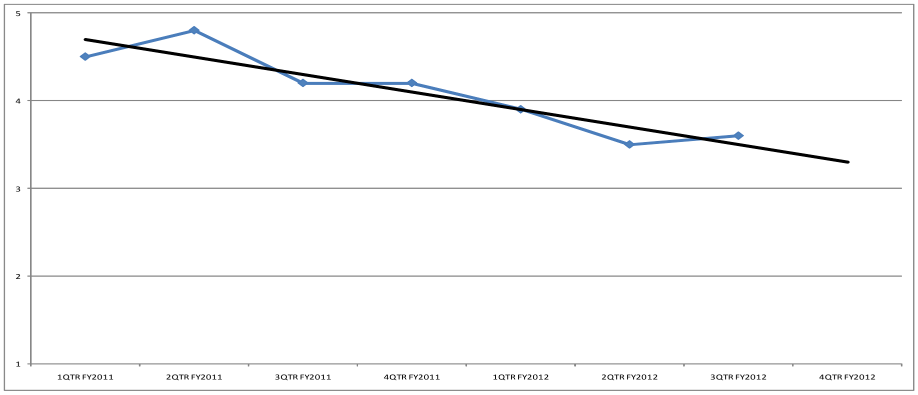


Figure 4. Security Posture Assessment Results over Time

ICSs Security Posture Data Calls

As a guide to help initiate a conversation within a Sector the following questions and initiatives should be discussed at the Sector Coordinating (or work group within it) level.

- What organization will conduct data calls?
- What should be the frequency of data calls?
- What is the format for data calls? (hopefully one format will work for all sectors)
- What is the policy on privacy of the data and how it will be used?
- Conduct a pilot test of data call with selected organizations to validate instructions and usefulness of data format
- Provide multiple channels for data calls including web sites, spreadsheets to make data collection easy.
- There should be validation of the data in the collection tools to enhance completeness and accuracy.
- Conduct training sessions on data calls and the importance of assessing security posture.
- Establish security around the data call information.

5. CROSS-SECTOR ROADMAP IMPLEMENTATION

This Cross-Sector roadmap contains a structured set of priorities that address specific control systems needs over the next 10 years. Individual CIKR sectors should consider the alignment of their sector specific roadmap to this cross-sector roadmap and what any gaps may mean to the sector. The objective of this coordinated approach is clearly defined activities, projects, and initiatives that contain time-based deliverables tied to roadmap goals and milestones.

- Draft Roadmap.
- The ICSJWG Roadmap Subgroup will seek approval of a charter revision to extend its work to implement the developed draft roadmap.
- The ICSJWG Road map Subgroup will obtain Sector Coordinating Councils input to the cross-sector roadmap.
- Document Common threads for ICS Challenges, priorities, and objectives across all Infrastructure Sectors.
- Prepare Gap Analysis for areas that need to be addressed.
    - This can lead to possible best practices where one sector is performing something that others may wish to or represent an area where a sector is working that may not be as beneficial.

Periodic roadmap implementation workshops organized by the ICSJWG Roadmap Subgroup will inform the ICSJWG and Sector SCC's progress towards goals and milestones, provide awareness training, and solicit new ideas for the activities supporting the milestones in Section 3. Government agencies should consider aligning resources and funding of priorities per the elements outlined within the roadmap because these priorities often focus on long-term needs or efforts that provide limited incentive for business investment. DHS CSSP should coordinate with the SCC in providing subject matter expertise supporting these workshops.

IMPLEMENTATION CHALLENGES

The ICSs security enhancement elements laid out by this roadmap are voluntary and specifically avoid recommending regulation to impose these priorities and actions on owners/operators and vendors.

Instead, as a result of continuing cyber attacks and threats against critical infrastructure, anticipated future ICSs security enhancements will be incorporated into each system's life cycle per a cost-benefit analysis of implementing risk mitigation measures.

The difficulty in developing the business case arises from the evolutionary nature of cyber systems—there is no long-term experience to project valid attack rate estimates. Quantifying the types of significant CIKR attacks is also a challenge—the feared attack is expected to be an extremely rare event with extremely high impact costs. This difficulty in estimating the probability and consequence parameters to arrive at an economic risk (expected loss) is further exacerbated by the technical complexity of integrated cyber control system information. The milestones and priorities for Goal 1 enhance understanding of system assessments, risk assessments, and analyses to ultimately result in a reliable business case resolving the challenge, i.e., justify voluntary investment in necessary cybersecurity enhancement.

The challenge is to stimulate voluntary efforts aggressively and productively. The Goals have been identified, in part, to help successfully implement this roadmap. They begin with awareness, risk analysis, and self assessment; and strive for long term, cost efficient technical solutions developed and provided by cyber control system vendors.

To help sustain this roadmap effort, the risk management planning process must include constant exploration of emerging ICSs security capabilities, vulnerabilities, consequences and threats.

PROPOSED OVERSIGHT MECHANISM

This roadmap encourages organizations to participate in ways that will best capitalize on their distinct skills, capabilities, and resources for improving the security of ICSs. This affords companies and organizations the flexibility to pursue projects aligned with their special interests. The rest of this section outlines the minimum efforts needed to effectively implement this roadmap.

ACTIVITY IMPLEMENTATION

The following steps implement the milestones, including policy development, partnership formation, training initiatives and R&D efforts. The roadmap workgroup provides project coordination of roadmap activities and takes the lead in carrying out ongoing implementation activities in three areas: collaboration, project coordination, and roadmap assessment.

COLLABORATION

The ICSJWG Roadmap subgroup will provide venues for collaboration efforts, ensure the tools being developed enable the secure sharing of information (such as a shared web site for monitoring activities), and promote ongoing information exchange on best practices and industry developments. The workgroup may also facilitate defining roles and responsibilities of critical infrastructure stakeholders.

PROJECT COORDINATION

The workgroup will take on a leadership role coordinating roadmap activities by assisting in defining roles, and identifying, initiating and tracking projects. Initially it will map current activities to roadmap milestones and goals, identify gaps, and initiate specific activities to fill the gaps. The workgroup will help to delegate tasks and subsequently track their progress meeting roadmap milestones.

ROADMAP ASSESSMENT

Project assessment involves the assessment and feedback of roadmap activities to assure they remain on target. In addition, it includes assessment of industry developments in ICSs and IT, and evolving security threats that may affect roadmap activities or require readjustments of goals, milestones and activities. Tracking these changes, the workgroup may recommend a revision of the roadmap if the developments are significant.

INFORMATION SHARING

Effective information sharing and awareness efforts help ensure the successful coordination and implementation of programs for protection of cyber assets, systems, networks, and functions. These efforts also enable informed decisions regarding short- and long-term cybersecurity posture, risk mitigation, and operational continuity.

Determining effective methods for sharing information within a sector, or across sectors, is a significant challenge for sector management. There must be a reliable means for disseminating information, ensuring the capability to receive information to protect ICSs.

The roadmap and the efforts of the ICSJWG Information Sharing Workgroup are excellent examples of outreach and information sharing. They increase the sector's situational awareness and provide suggestions focused on the reduction of potential consequences associated with cyber threats to ICSs.

ONGOING PROCESSES

Logistical assistance will be required to support meetings, including adequate meeting space, facilitation, and workshops to provide needed continuity for roadmap efforts. Collaboration tools, such as separate electronic space, teleconference meetings, and web-based meetings should be included.

Initially, implementation phases occur consecutively. Over time, the implementation must transition to an ongoing process that usually includes revisions to both the milestones and the goals. Ultimately, the roadmap implementation becomes indistinguishable from the sectors' ongoing CIKR protection efforts. The roadmap adds greatest value as an instrument of collaboration and a focal point for action within CIKR overall security efforts.

The roadmap will continue to evolve as industry reacts to business pressures, cyber threats, operational constraints, societal demands, and unanticipated events. While it does not cover all pathways to the future, implementation of effective programs to achieve roadmap goals and vision provides focus on what the sector believes to be a sound approach to address the most significant ICSs challenges:

- A cross-sector specific baseline ICSs security posture
- An effective communications and outreach strategy
- Training and appropriate certification

The roadmap is intended to guide planning and implementation of collaborative cybersecurity programs involving owners and operators, industry associations, government, commercial entities, and researchers in a nationwide effort to improve ICSs security.

KEY STAKEHOLDERS

Control systems security is a shared responsibility among asset owners, vendors, and stakeholders using ICSs to control processes and manage and govern CIKR assets. The control systems stakeholder community also includes government agencies, industry organizations, commercial entities, and researchers. Each brings specialized skills and capabilities for improving control system security and protecting CIKR. Key stakeholder groups and sample members include:

- *Asset owners and operators* ensure that control systems are secure by making the appropriate investments, reporting threat information to the government, and implementing protective practices and procedures
- *System and software vendors and system integrators*, develop and deliver control system products and services to meet the security needs of asset owners and operators
- *Federal, state, local, tribal, and territorial agencies* securely share threat information and collaborate with industry to identify and fund gaps in ICSs security research, development, and testing efforts
- *Industry organizations* provide coordination and leadership across multiple sectors to help address important barriers, form partnerships, and help to develop standards and guidelines specific to the needs of their sector membership
- *R&D organizations,* funded by government and industry, explore long-term security solutions, develop new tools, and address solutions for ICSs vulnerabilities, hardware, and software.

- *Universities and colleges,* chartered to provide education for future generations, ideally provide courses and degrees that satisfy the needs and requests of industry.

ROLES AND RESPONSIBILITIES

The responsibility for cybersecurity spans all public and private sector CIKR partners, due to the interconnected nature of the cyber infrastructure. Cyber infrastructure enables all sectors' functions and services, resulting in a highly interconnected and interdependent global network of CIKR. The protection of physical and cyber assets separately is not a realistic option.

This section contains primary roles and responsibilities of the various sector security partners for the coordination, refinement, and execution of the overarching CIKR Sector protective program. The following list of responsibilities is not specifically associated with particular programs, projects, or funding; and does not constitute a commitment by a specific company, organization, or government agency.

- Roadmap Implementation Committee:
    - The Roadmap Implementation Committee will support roadmap projects and cybersecurity initiatives promoted or tracked by the SCC. This includes electronically publishing and tracking deliverables and outcomes of projects, providing feedback, and electronic posting of information sharing and awareness topics addressed in the roadmap milestones not otherwise provided in related information sharing outlets. The committee will hold, host, support, and/or organize periodic meetings for interested parties to define projects and solicit new proposals and concepts.
    - If the Roadmap Implementation Committee determines that a particular roadmap milestone or newly identified gap in the path to the roadmap vision is not being addressed through adequate ongoing efforts, the issue will be brought to the attention of the SCC. Requests will then be sent to the stakeholders stating the problem and seeking their support including the planning and prioritizing of projects, and most importantly, funding for initiatives to address known gaps. This support may be directed toward basic research, applied research, technology commercialization, product integration, field-testing, scaled roll-out, training/outreach, or any other means or method that advances a particular milestone.
- DHS:
    - Work with Sector stakeholders to identify CIKR protection priorities for the CIKR Sectors
    - Provide information for protective program decisions
    - Work with the ICSJWG to coordinate deployment of Federal resources and minimize duplication of efforts
    - Support state, local, tribal, and private sector efforts by sharing threat information and issuing warnings.
- Non-DHS FEDERAL entities:
    - Provide information for informed protective program decisions
    - Review protective measures implemented by infrastructure owners and operators
    - Support international efforts to strengthen the protection of CIKR.
- State, local, tribal, and territorial governments:

    - Supplement DHS protective security guidance to the private sector within their communities
    - Provide National Guard, state and local law enforcement personnel, and other resources as needed in response to specific threat information and successful attacks.
- Private sector owners/operators:
    - Interact with DHS (US-CERT and ICS-CERT) to take advantage of available threat, incident, and vulnerability information
    - Implement site-specific protective measures
    - Participate in identifying accepted industry practices
    - Report cyber incidents or newly discovered vulnerabilities to the US-CERT at http://www.us-cert.gov/control_systems/
    - Share information within the CIKR Sectors and FEDERAL agencies as required.
- Universities and colleges:
    - Develop cyber control systems security courses.
    - Establish cyber control systems security degree programs
    - Support the establishment and awarding of scholarships, fellowships, research assistantships, and other student financial support mechanisms.

CYBERSECURITY BUSINESS CASE

OVERVIEW

Cybersecurity is becoming increasingly significant with regards to safeguarding information and control networks from penetration and malicious damage and/or disruption. Industrial Control Systems are essential for optimal business performance and alignment with organization risk expectations and requirements. The need to protect these critical systems is usually driven by escalating costs of productions loss associated with a cyber event.

Efficient and uninterrupted operational system performance is essential to the ability of an organization to meet the needs of its customer base, shareholders and/or regulatory agencies. In addition, corporation value is determined, in many cases, on just how efficient and operation can run admits the potential intrusions of cyber attacks.

As organizations seek methods of defending their business and control systems against cyber attack, questions continue to arise with regards to the costs associated with establishing layers of defense. Enhancing the cybersecurity of an organization may often require significant resources and funding in the areas of training, equipment/software upgrades and policy changes. The choice to allocate resources and funding for cybersecurity must be evaluated to determine the costs and benefits associated with any expenditure.

Justification for cybersecurity improvement and enhancement starts with developing a business case that carefully explores the financial risks and consequences a cyber event. Business cases are forward looking documents directly involved in long term planning and contain prediction and inherent uncertainty. However, the uncertainty about the likelihood of a cyber event or the overall and potential hidden costs associated with such an event should not diminish the need for establishing a credible business case that address the needs of physical and culture changes.

BUILDING A CYBERSECURITY BUSINESS CASE

Building a business case will not eliminate all uncertainty from predicted results but will focus an organization to understand and organize knowledge of potential risk and costs. A best attempt should be made to minimize uncertainty and measure what remains. Cost models and risk analysis can be used to show all relevant costs associated with predicted results. A suggested flow process for developing a business case is shown in Figure 1. The use of the DHS's Cyber Security Evaluation Tool (CSET) is listed as a suggested method for evaluating an organizations current cybersecurity posture. CSET can be used in the development of business cases, cybersecurity plan and/or business policies and procedures.

Numerous organizations and agencies have reported cyberattacks are becoming more frequent and are having significant impacts on the corporate bottom line. "In a poll sponsored by a cyber risk management firm ArcSight, Ponemon surveyed security professionals in 45 US organizations. Over a four-week period those organizations experienced 50 successful attacks per week, or more than a successful attack per organization per week. The median annual cost per organization per year was $3.8 million. The smallest loss was $1 million; the biggest, nearly $52 million. Every organization is vulnerable to numerous cyber attacks that occur daily across all industries, causing information theft, business disruption and serious financial loss." Cyberattacks Hit Bottom Line, by Jefferson Graham, USA Today July 28, 2010.

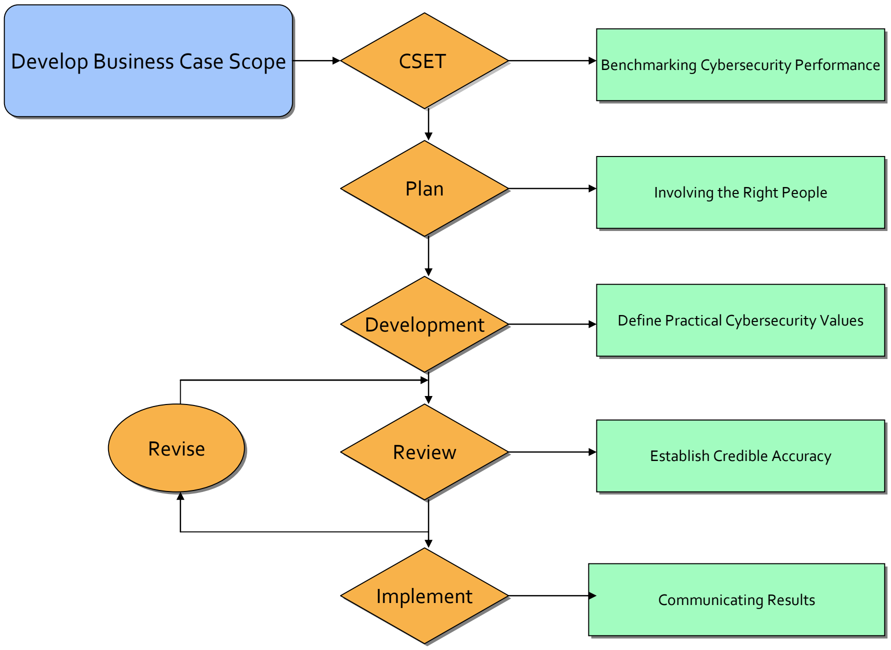

Develop Business Case Scope
CSET
Benchmarking Cybersecurity Performance
Plan
Involving the Right People
Development
Define Practical Cybersecurity Values
Revise
Review
Establish Credible Accuracy
Implement
Communicating Results

Figure 5. Business Case Development

POTENTIAL CYBERSECURITY THREATS

Threats to control systems can originate from various sources, including adversarial organizations or governments, terrorists groups, industrial spies, malicious intruders or disgruntled employees. Known threats are listed in Table 2. This list is not all inclusive but provides a description some key threats to cyber networks.

Potential Threat	Description
Criminal Groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the U.S. through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop attacker talent. Some criminal groups may try to extort money from an organization by threatening a cyber attack
Insider	The disgruntled insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems. Insiders may be employees, contractors, or business partners. Inadequate policies, procedures, and testing can, and have led to ICS impacts. Impacts have ranged from trivial to significant damage to the ICS and field devices. Unintentional impacts from insiders are some of the highest probability occurrences.
Phishers	Phishers are individuals or small groups that execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Spammers are individuals or organizations that distribute unsolicited email with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (e.g., DoS).
Spyware/Malware	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware to generate funds or gather sensitive information. Terrorists may attack one target to divert attention or resources from other targets.
Industrial Spies	Industrial espionage seeks to acquire intellectual property and know-how by clandestine methods.

Table 2. Potential Cyber Threats

PRIORITIZED BUSINESS CONSEQUENCES

A list of potential business consequences should be developed consistent with the operational criteria of a particular organization and those that senior management will find the most applicable and compelling. In what cases regulatory compliance is a concern, attention should be given to consequences associated with not being able to achieve regulatory compliance. Some of these consequences may include:

- Loss of production
- Employee injuries
- Equipment damage
- Release, diversion or theft of hazardous materials
- Environmental damage
- Violation of regulatory requirements
- Product contamination
- Criminal or civil legal liabilities
- Loss of proprietary or confidential information
- Loss of brand image or customer confidence

PRIORITIZED BUSINESS BENEFITS

Improved control systems security and control system specific security policies can potentially improve control system reliability and availability. Enhanced security policies provide positive benefit of minimizing unintentional control system cyber security impacts from inappropriate testing, policies, and misconfigured systems. Some of the benefits associated with implementation of a comprehensive cybersecurity plan include:

- Improving production performance and reducing downtime
- Reduce third-party reliance
- Reduce regulatory fines
- Reduce network maintenance costs
- Improving ability to detect and mitigate cyber intruders
- Increase awareness
- Enhance response time to cyber event

ESTIMATED ANNUAL BUSINESS IMPACTS

The highest priority items identified in the list of prioritized business consequences should be evaluated to obtain an estimate of the annual business impact, preferably but not necessarily in financial terms. An organization may have experienced a virus incident within its internal network that the information security staff estimated as resulting in a specific financial cost. If the internal network and the control network are interconnected, a virus originating from the control network could cause the same amount of business impact.

KEY ELEMENTS OF A CYBERSECURITY BUSINESS CASE

This section will address:

- What are the key elements to a business case?
- What makes it compelling and credible?
- Are there standards and rules for a business case structure and content?

Businesses are becoming more and more driven to make accountable decisions based on financial objectivity. Throughout corporate environments the competition for scarce funds is becoming more intense. The need to develop a compelling cybersecurity business case is essential but few organizations have established and implemented one.

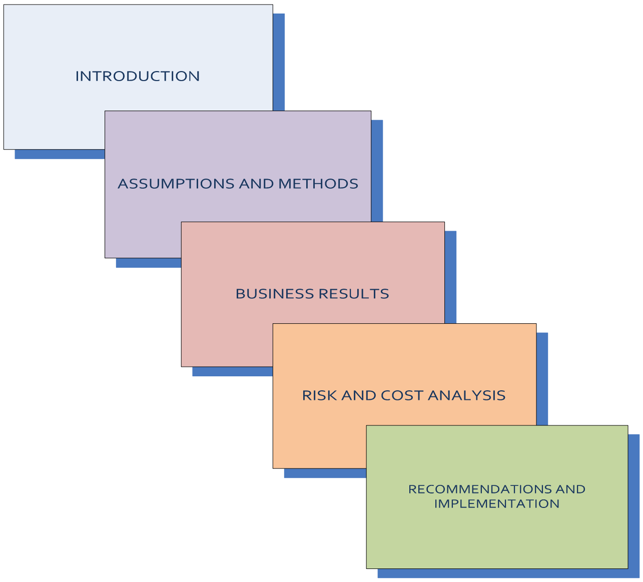


Figure 6. Business Case Key Elements

INTRODUCTION

The entire business case follows from an effectively described subject and purpose as introduced in the introduction section. This section should be expanded to discuss the proposed actions and business objective associated with strengthening the company's cybersecurity.

ASSUMPTIONS AND METHODS

The need to establish definable assumptions and effective methods are critical. Assumptions will include business type, market size, inflation rates, and component/equipment costs.

BUSINESS RESULTS

The overall results will support and indicate how each assumption contributes to the overall results. Results will include financial metrics (e.g., total costs, return on investment and/or payback period etc.)

RISK AND COST ANALYSIS

Risk and cost analysis provides a method for establishing the likelihood of other results instead of the primary predicted result. These types of analyses can provide the business case a kind of quality control for project, program and other business investments.

RECOMMENDATIONS AND IMPLEMENTATION

As with any type of "actionable" document, recommendations and a path for their implementation should adequately be described and evaluated. Considerations should be given to the current business situation and priorities associated with organizational policy and procedures.

Recommendations can include decision criteria necessary for effective results and financial and non-financial information for establishing baselines and timelines for establishing a practical conclusion.

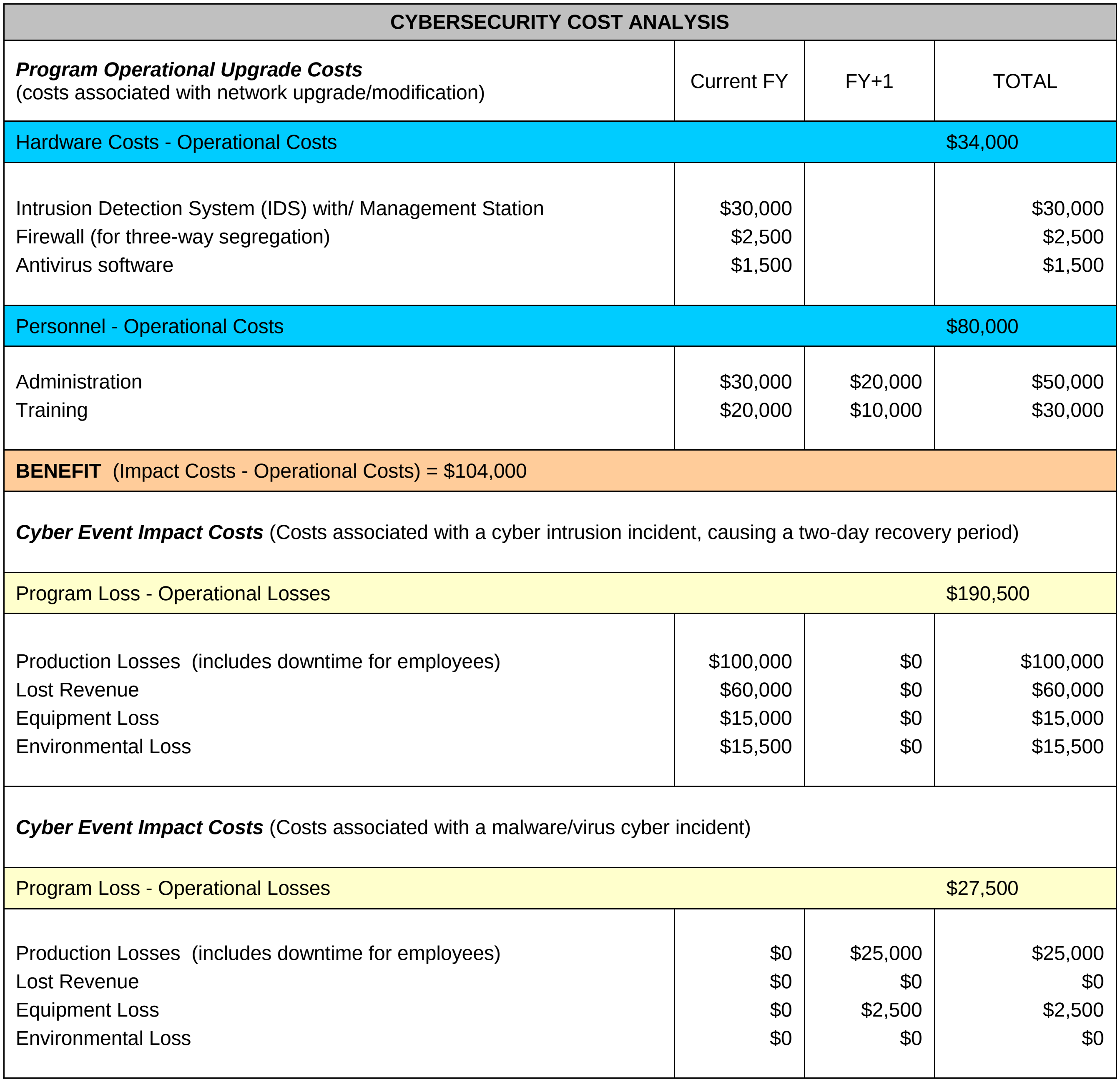
BUSINESS CASE ANALYSIS

Undesirable network incidents on any level can detract from the value of an organization by loss of production, loss of information, damage to equipment and seemingly undermine consumer confidence. As such, establishing key components within a formalized cybersecurity business case is essential. These components include, but are not limited to: identified and prioritized threats, prioritized business consequences, prioritized business benefits and estimated annual business impacts.

The scenario shown in Figure 3, represents a cyber intrusion event, during year one and a malware/virus disturbance during year two, that could cause a two-day system wide impact. The event is estimated to take approximately two days to fully recover from a cyber intrusion event such that all equipment and systems have been properly evaluated, sanitized and upgraded so as to mitigate any effects of the event. In addition, in year two a malware/virus disturbance was encountered causing additional system impacts. The two events combined suggest an overall cost for recovery at $218K.

With respect to developing a defense in depth strategy, the capital expenditures identified in Figure 3, suggest several modification/enhancements to an organization's cybersecurity posture so as to mitigate potential intrusions and/or disturbances within the organizations cyber network. The overall costs associated with these modifications are identified to be $114K

When operational costs are subtracted from the impact costs, the remainder illustrates the overall benefit for implementing these security upgrades as $104K. Each organization may identify additional or different organizational costs as well as impact costs, thereby greatly expanding their cost analysis. This scenario provides a simple example cost comparisons.



CYBERSECURITY COST ANALYSIS			
Program Operational Upgrade Costs (costs associated with network upgrade/modification)	Current FY	FY+1	TOTAL
Hardware Costs - Operational Costs			$34,000
Intrusion Detection System (IDS) with/ Management Station	$30,000		$30,000
Firewall (for three-way segregation)	$2,500		$2,500
Antivirus software	$1,500		$1,500
Personnel - Operational Costs			$80,000
Administration	$30,000	$20,000	$50,000
Training	$20,000	$10,000	$30,000
BENEFIT (Impact Costs - Operational Costs) = $104,000			
Cyber Event Impact Costs (Costs associated with a cyber intrusion incident, causing a two-day recovery period)			
Program Loss - Operational Losses			$190,500
Production Losses (includes downtime for employees)	$100,000	$0	$100,000
Lost Revenue	$60,000	$0	$60,000
Equipment Loss	$15,000	$0	$15,000
Environmental Loss	$15,500	$0	$15,500
Cyber Event Impact Costs (Costs associated with a malware/virus cyber incident)			
Program Loss - Operational Losses			$27,500
Production Losses (includes downtime for employees)	$0	$25,000	$25,000
Lost Revenue	$0	$0	$0
Equipment Loss	$0	$2,500	$2,500
Environmental Loss	$0	$0	$0

Figure 7. Cost Analysis

SUMMARY

Business case developer and review personnel may have varying levels of knowledge about what to look for in establishing a credible business case. Determining arguments through analysis that are strongest to enhance cybersecurity may be challenging. In all cases, however, any business case development effort should be future oriented and predictions about future events contain inherent uncertainty.

No single correct outline or method for the business case exists, but all good cases have the essential key elements included. The business case, with proposed actions, will provide valuable information necessary to make decisions that will positively affect the posture of an organization’s cybersecurity and further expand the layers-of-defense established to mitigate vulnerabilities.

6. References

1. Department of Homeland Security, National Infrastructure Protection Plan, 2006.
2. NIST Special Publication 800-82, FINAL PUBLIC DRAFT, Keith Stouffer, Joe Falco, Karen Scarfone, September 2008.

A. National Policy Guidance on Cyber Control System Security

In 1988 Presidential Decision Directive NSC-63 (PDD-63), "Critical Infrastructure Protection," was issued recognizing the need for enhanced security of the nation's cyber aspects of critical infrastructure. Although directed specifically to information systems, it recognized the interdependencies within the critical infrastructure sectors and the reliance of that infrastructure on automated, cyber systems. The directive called for voluntary private-public partnerships of the type formalized in the National Infrastructure Protection Plan (NIPP), provided an assignment of government agencies as lead sector agencies, and called for the creation of private sector information sharing and analysis center, which evolved into the Sector Information Systems Advisory Councils.

Federal Information Security Management Act of 2002 requires that Federal agencies develop a comprehensive information technology security program to ensure the effectiveness of information security controls over information resources that support Federal operations and assets. This legislation is relevant to the part of the NIPP that governs the protection of Federal assets and the implementation of cyber-protective measures under the Government Facilities Sector-Specific Plan.

The *Cybersecurity Research and Development Act of 2002* allocates funding to National Institute of Standards and Technology and the National Science Foundation for the purpose of facilitating increased research and development (R&D) for computer network security and supporting research fellowships and training. The act establishes a means of enhancing basic R&D related to improving the cybersecurity of CIKR.

The *National Strategy for Homeland Security* and the *Homeland Security Act of 2002* responded to the attacks of 9/11 by creating the policy framework for addressing homeland security needs and restructuring government activities, which resulted in the creation of Department of Homeland Security (DHS).

In early 2003, the *National Strategy to Secure Cyberspace* outlined priorities for protecting against cyber threats and the damage they can cause. It called for DHS and DOE to work in partnership with industry to "... develop best practices and new technology to increase security of DCS/SCADA, to determine the most critical DCS/SCADA-related sites, and to develop a prioritized plan for short-term cybersecurity improvements in those sites."

In late 2003, the President issued Homeland Security Presidential Decision 7 (HSPD-7)**,** "Critical Infrastructure Identification, Prioritization, and Protection," to implement Federal policies. HSPD-7 outlined how government will coordinate for critical infrastructure protection and assigned DOE the task of working with the energy sector to improve physical and cybersecurity in conjunction with DHS. Responsibilities include collaborating with all government agencies and the private sector, facilitating vulnerability assessments of the sector, and encouraging risk management strategies to protect against and mitigate the effects of attacks. HSPD-7 also called for a national plan to implement critical infrastructure protection.

Executive Order 13231 (as amended by E.O. 13286 of February 28, 2003 and E.O. 13385 of September 29, 2005) established the National Infrastructure Advisory Council (NIAC) as the President's principal advisory panel on critical infrastructure protection issues spanning all sectors. The NIAC is composed of not more than 30 members, appointed by the President, who are selected from the private sector, academia, and state and local government, representing senior executive leadership expertise from the CIKR' areas as delineated in HSPD-7. The NIAC provides the President, through the Secretary of

Homeland Security, with advice on the security of critical infrastructure, both physical and cyber. The NIAC is charged to improve the cooperation and partnership between the public and private sectors in securing critical infrastructure and advises on policies and strategies that range from risk assessment and management, to information sharing, to protective strategies and clarification on roles and responsibilities between public and private sectors.

B. GUIDING AND ALIGNING EXISTING EFFORTS

As discussed in Section 2 and summarized in Table B-1 below, a significant effort to enhance control system security is already underway. These organizations and efforts provide a starting point from which to support the achievement of goals and milestones presented in this roadmap.

Table B-1- Selected Control System Security Efforts

Activity	Lead Organization	Scope	Major Actions and Events
Industrial Control System Joint Working Group (ICSJWG)	DHS Office of Infrastructure Protection and the Critical Infrastructure Partnership Advisory Council	Coordinate Federal, State, and private sector initiatives to secure ICSs	• ICSJWG half yearly and annual meetings.
Institute for Information Infrastructure Protection (I3P)	Dartmouth College, DHS Science and Technology Directorate, and NIST	National cybersecurity R&D coordination program	• I3P SCADA Security Research Project launched (2005) • I3P Research Report No. 1: *Process Control System Security Metrics* (2005) • *Securing Control Systems in the Oil and Gas Infrastructure, The I3P SCADA Security Research Project* (2005)
Control Systems Security Program	DHS National Cyber Security Division, INL, and U.S. Computer Emergency Readiness Team (US-CERT)	Testing and Information Center for control systems cybersecurity	• Created and operates the ICS-Cyber Emergency Response Team (ICS-CERT) • Initiated the ICS Joint Working Group (ICSJWG) in December 2008 • Operates cyber vulnerability testing and assessment capabilities for installed control systems and vendor components • Develops risk analysis and self-assessment tools

Activity	Lead Organization	Scope	Major Actions and Events
ISA-99 Committee	ISA	The ISA-99 Committee addresses manufacturing and control systems whose compromise could result in any or all of the following situations: • Endangerment of public or employee safety • Loss of public confidence • Violation of regulatory requirements • Loss of proprietary or confidential information • Economic loss • Impact on national security	The committee has produced the following work products: • ANSI/ISA-TR99.00.01-2007, *Security Technologies for Manufacturing and Control Systems (2007)* • ANSI/ISA-99.00.01-2007, *Security for Industrial Automation and Control Systems: Concepts, Terminology and Models* • ANSI/ISA-99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program* The current emphasis is on addressing the topic "Technical Requirements for Industrial Automation and Control Systems." Working Group 4 will produce a series of standards and technical reports on this topic. The committee holds weekly working group meetings as well as general sessions at ISA Automation Week (annually).
ISA Security Compliance Institute	ISA	Ensure that industrial control system products and services comply with industry standards and practices, "Development of tests specifications and methodologies based on available standards and practices"	• ISA Security Compliance Institute Formal Launch – January 2008 • Certification Program Operations, Polices, and Processes Complete – November 2008 • Certification Program Complete – Operational December 2010