Roadmap to Secure Control Systems in the Chemical Sector

September 2009

Homeland Security

This page intentionally left blank

Roadmap to Secure Control Systems in the Chemical Sector

Prepared by the
Chemical Sector Roadmap Working Group

Sponsored by the
U.S. Department of Homeland Security and the
Chemical Sector Coordinating Council

September 2009

This page intentionally left blank

FOREWORD

The Roadmap to Secure Control Systems in the Chemical Sector describes a plan for voluntarily improving cybersecurity in the Chemical Sector. Sector roadmaps provide an opportunity for industry experts to offer input concerning the state of control systems cybersecurity and to communicate recommended strategies for improvement within their sector. This roadmap brings together Chemical 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 over the next 10 years, while addressing the Chemical Sector's most urgent challenges, longer-term needs, and practices to reduce the cybersecurity risk to industrial control systems (ICS).

The U.S. Department of Homeland Security's (DHS) Office of Infrastructure Protection (IP) and the National Cyber Security Division (NCSD) facilitated the development of this roadmap, with volunteers from Chemical Sector 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 ICS within the Chemical Sector.

CHEMICAL SECTOR ROADMAP WORKING GROUP

Esther Abelman (Energetics, Inc., in support of DHS)

Marc Ayala (AkzoNobel)

George Beitel (Performance Results Corporation, Technical Writer)

Michael Butler (Dow Chemical)

Eric Cosman (Dow Chemical)

Terry Deo (Infineum)

Tom Good (DuPont)

Amy Graydon (DHS, Chemical Sector-Specific Agency)

Mark Heard (Eastman Chemical)

Blake Larson (Western Refining)

Sean Paul McGurk (DHS, Control Systems Security Program)

Baird McNaught (Idaho National Laboratory support to DHS, Control Systems Security Program)

Johan Nye (ExxonMobil)

Julio Rodriguez (Idaho National Laboratory support to DHS, Control Systems Security Program)

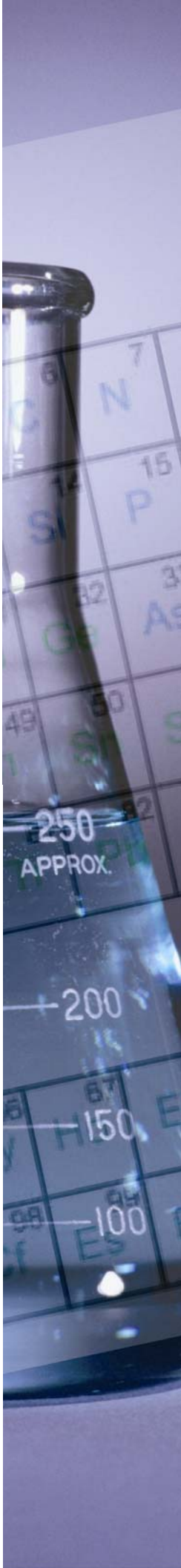
Steve Salvo (Air Products)

Mike Sauer (Ashland)

Jonathan Schreiter (Air Products)

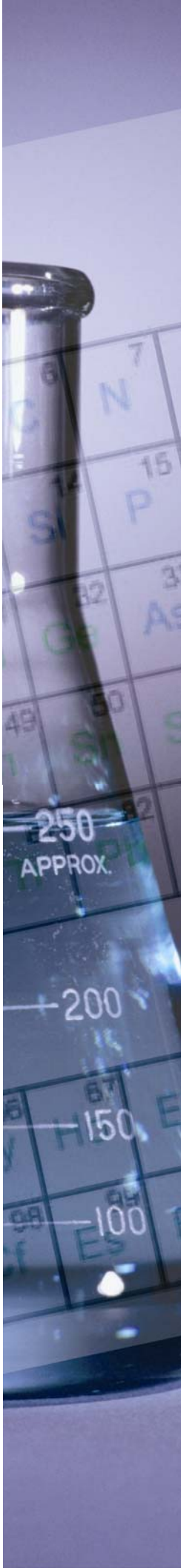
Dan Strachan (National Petrochemical & Refiners Association)

Steve Tippet (ExxonMobil)



This page intentionally left blank

CONTENTS



This page intentionally left blank

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 critical infrastructure asset owners in reducing the risk of future cyber attacks on control systems.

In recent years, roadmaps[1,2] have been developed to guide the efforts of individual sectors in securing their industrial control systems (ICS). 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 U.S. Department of Homeland Security (DHS) is leveraging this industry perspective to help the sector stakeholder community develop programs and risk mitigation measures that align with the sector's plan. In addition to the asset owners and operators, other sector stakeholders include 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 organization's overall cybersecurity policies and procedures. Still, roadmaps are recognized as quality documents that provide excellent descriptions of control systems risk challenges and general methods for improving the security of control systems over the ensuing decade.

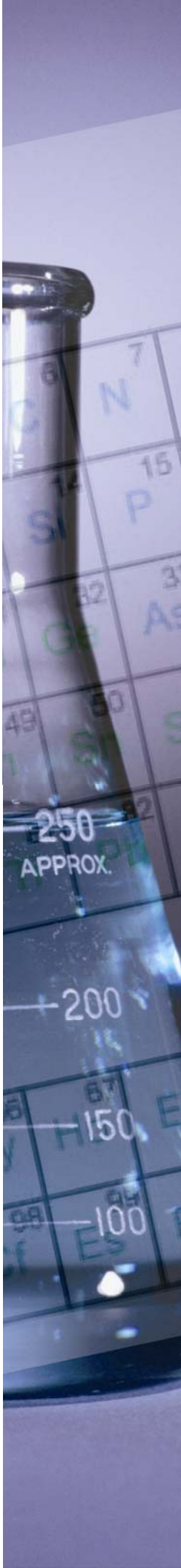
The specific challenges, goals, and priorities of the Chemical Sector are detailed in Section 3 of this roadmap.

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), Industrial Control System Joint Working Group (ICSJWG), Process Control Security Requirements Forum (PCSRF), and academic institutes supporting the Chemical Sector. This roadmap:

Roadmap Purpose

- Present the Chemical Sector's security vision
- Define a consensus-based strategy for the sector
- Propose a comprehensive plan to improve security
- Encourage stakeholder participation and compliance
- Guide industry, academia, and government effort
- Identify opportunities for cross-sector cooperation
- Promote continuous improvement in security posture



- Presents a vision, along with a supporting framework of goals and milestones, to improve the cybersecurity posture of ICS within the sector;
- Defines a consensus-based strategy that addresses the specific cybersecurity needs of owners and operators of Critical Infrastructure and Key Resource (CIKR) facilities;
- Proposes a comprehensive plan for improving the availability, security, reliability, and functionality of ICS over the next 10 years;
- 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; and
- Promotes continuous improvement in the security posture of ICS within CIKR sectors.

ROADMAP SCOPE

This roadmap addresses cybersecurity issues related specifically to ICS owned and operated by chemical industries whose facilities are part of the Nation's CIKR. The functional and organizational composition of CIKR sectors is defined in the National Infrastructure Protection Plan (NIPP)[3] and subordinate Sector-Specific Plans (SSPs). Vendors that supply and maintain cyber control components and systems are an integral part of the cyber control system problem-solution space encompassed by this roadmap.[a]

Designing, operating, and maintaining a facility to meet essential availability, reliability, safety, and security needs requires the careful evaluation and analysis of all risk factors, including physical, cyber, and human. The interaction of both internal and external process and business systems must also be considered. 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 ICS.[b] 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 risks to ICS encompass elements of the business network and Internet to the extent they are connected to process control systems. While security for IT systems is outside the scope of this roadmap, interfaces between the ICS networks, business system networks, and Internet connections must be coordinated to ensure proper application of security measures and responsibilities.

---

a. The Chemical Sector is bounded by the definition contained within the NIPP.[3] The sector definitions within the NIPP result in companies, and even facilities, that are in more than one sector. For example, the Chemical Sector overlaps with the Energy Sector, particularly in the area of petroleum.

b. 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, and distributed control systems. It does not cover business or information systems.

Physical access to cyber systems is a significant contributing factor in addressing cyber risk. Similarly, physical damage resulting from cyber compromise is one of the principal factors contributing to 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 is outside 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. The Roadmap will be updated periodically to meet changing needs and to accommodate the dynamic nature of cybersecurity for control systems.

NATIONAL CONTEXT

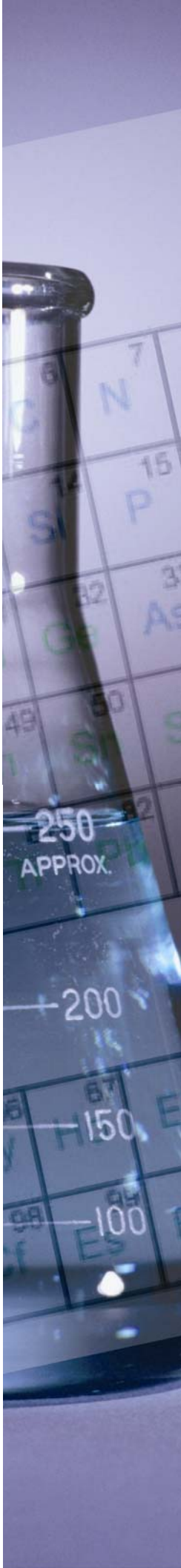
The NIPP and Homeland Security Presidential Directive 7 (HSPD-7)[4] establish a partnership model for collaboration that consists of a Sector Coordinating Council (SCC), a Government Coordinating Council (GCC), and an assigned Sector-Specific Agency (SSA; a Federal agency) for each CIKR sector. The SSA, among other things, collaborates with Federal, State, local, tribal, territorial, and private sector partners to encourage the development of information sharing and analysis mechanisms. The SSA also facilitates the sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and accepted 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. The Chemical Sector Roadmap Working Group was developed out of the Chemical SCC and GCC.

In 2004, the DHS National Cyber Security Division (NCSD) established the Control Systems Security Program (CSSP), which is chartered to work with control systems security stakeholders through awareness and outreach programs that encourage and support coordinated control systems security enhancement efforts. As a member of the Chemical GCC, CSSP is working in collaboration with the Office of Infrastructure Protection in the development of this roadmap. In December 2008, the CSSP also established the ICSJWG as a coordination body to facilitate the collaboration of control systems stakeholders and to accelerate the design, development, and deployment of enhanced security for control systems.

This roadmap recommends the implementation of Federal policies that encourage Federal agencies to collaborate with industry to create a national strategy that reflects the needs and expectations of both government and industry. Roadmap priorities and recommendations help inform and strengthen government programs designed to improve the protection of ICS.

Appendix A summarizes national policy guidance on securing cyber control systems.



ACTION PLAN

This roadmap proposes a strategic framework for investing in control system security risk mitigation efforts and for industry and government action toward improving defenses against cyber events that would disrupt operations. It identifies the challenges and activities that should be addressed, and provides specific milestones that should be accomplished over the next 10 years to achieve the outlined goals and vision. While it contains many actionable items, as a plan, 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.

2. CONTROL SYSTEM LANDSCAPE

ICS perform various functions and exist at different stages of evolution throughout the Nation's CIKR. Many of the ICS used today were designed for availability and reliability during an era when cybersecurity 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 ICS are network-based and use common standards for communication protocols. Many controllers are Internet Protocol addressable. Asset owners and operators have gained immediate benefits by extending the connectivity of their ICS. 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 or UNIX are commonly used in central supervisory stations, 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 networks or satellite (wireless), and radio networks are often used to provide the telecommunication services. A typical ICS configuration is shown in Exhibit 1.

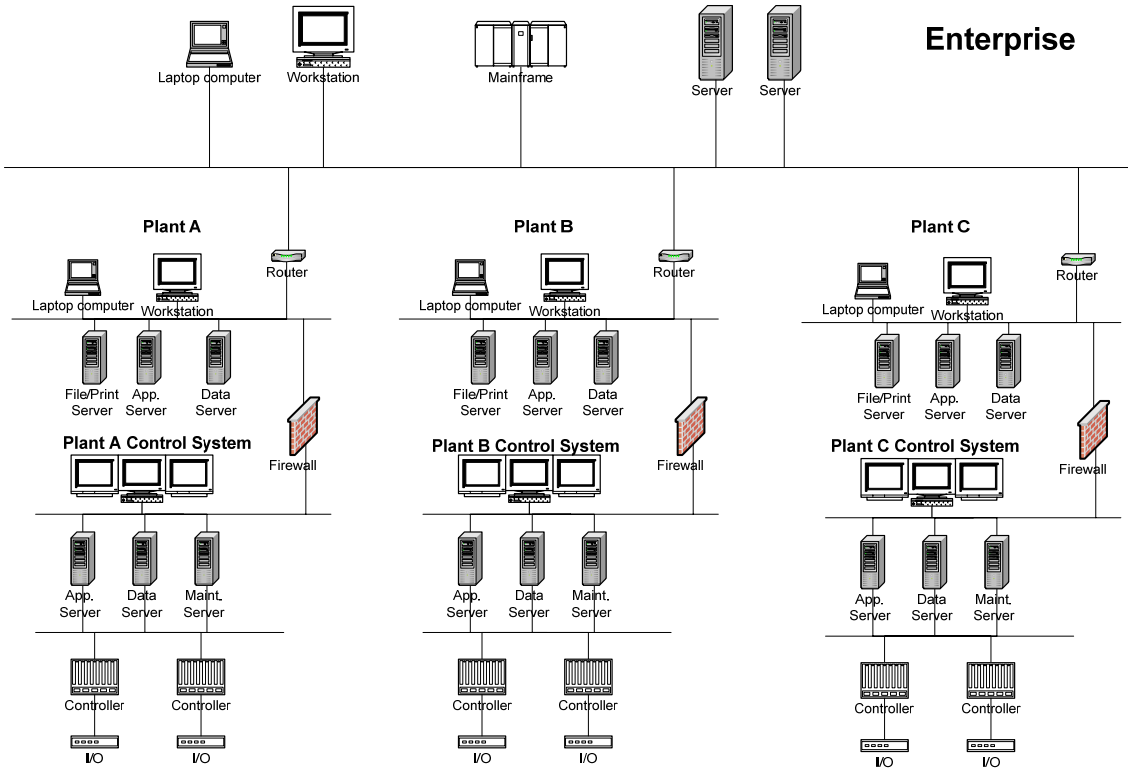


Exhibit 1. Typical ICS configuration[5]

The potential for system accessibility resulting from this interoperability exposes network assets to cyber 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 ICS are engineered for reliability, security policies and practices are often not up to date or compliant with current standards or practices. Detailed analyses of the potential threats and associated consequences are also lacking in some facilities.[6] As operating practices have evolved to allow real-time operation and control of critical assets, protecting ICS from cyber risks has become more difficult. Some of the most serious security issues facing current ICS applications are described below:

Security Issues

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

- ***Increased Connectivity***. Today's ICS are being increasingly connected to company business systems that rely on common operating platforms and are accessible through the Internet. Even though these changes improve operability, they also create 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 control has increased system complexity in several ways: access to ICS is being granted to more users, business and ICS 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 ICS 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 Accessibility.*** Even limited connection to the Internet exposes ICS 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.*** There are no feasible alternatives to the use of commercial off-the-shelf products in these ICS. Many software, hardware, and ICS 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 the support, service, and maintenance of ICS to third parties located in foreign countries.
- ***Information Availability.*** Manuals and training videos on ICS 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 ICS, their vulnerabilities, and other resources can be found on the U.S. Computer Emergency Readiness Team (US-CERT) Control System website at http://www.us-cert.gov/control_systems/csvuls.html, and the 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."[7]

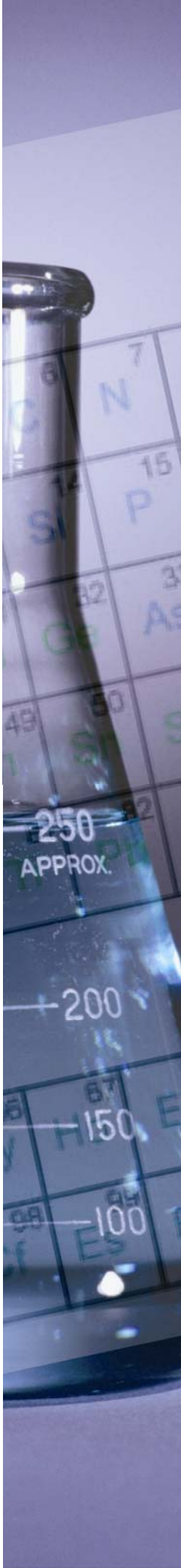
KEY STAKEHOLDERS

ICS security is a shared responsibility among asset owners, vendors, and stakeholders who manage and govern critical infrastructure assets. The ICS stakeholder community also includes government agencies, industry organizations, commercial entities, and researchers, each of which brings specialized skills and capabilities for improving control system security and protecting CIKR. Key stakeholder groups and sample members include:

- *Asset owners and operators* who ensure that ICS are secure by making the appropriate investments, reporting threat information to the government, and implementing protective practices and procedures
- *Federal, State, local, tribal, and territorial agencies* that securely share threat information and collaborate with industry to identify and fund gaps in ICS security research, development, and testing efforts
- *Industry organizations* that provide coordination and leadership across multiple sectors to help address important barriers, form partnerships, and develop standards and guidelines specific to the needs of their sector membership
- *Commercial entities*, such as system and software vendors and system integrators, that develop and deliver ICS products and services to meet the security needs of asset owners and operators
- *R&D organizations* funded by government and industry that explore long-term security solutions, develop new tools, and address solutions for ICS system vulnerabilities, hardware, and software
- *Universities and colleges* chartered to provide education for future generations that ideally provide courses and degrees that satisfy the needs and requests of industry.

A FRAMEWORK FOR SECURING CONTROL SYSTEMS

Protecting CIKR 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 a strategy to articulate the essential goals for improving ICS 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.

VISION

The vision of the Chemical Sector Roadmap Working Group is:

> *In 10 years, the layers of defense for industrial control systems managing critical applications will be designed, installed, and maintained, commensurate with risk, to operate with no loss of critical function during and after a cyber event.*

Two noteworthy points within the vision are "critical applications" and "commensurate with risk."

Critical applications are those with functions that if lost, could result in both immediate and long-term severe economic damage, environmental damage, public endangerment, including loss of life and loss of public confidence, and impact on governance. These are consequence categories specifically addressed and defined in the NIPP, which adds "environmental damage" for emphasis.

The "commensurate with risk" point in the vision statement provides for a metric to determine how much improvement is enough. Risk is the measure of the integration of the probability of a cyber attack and its consequences. The intent of the vision is to enhance security to a level at which risk is acceptable and at a low enough cost to enable industry to function in a cost-efficient manner. An effective risk assessment includes both the immediate losses and indirect impacts of a cyber intrusion or attack and the fully explored ramifications as a loss of control incident propagates through multi-industry and multi-sector interactions.

CONTROL SYSTEMS SECURITY GOALS

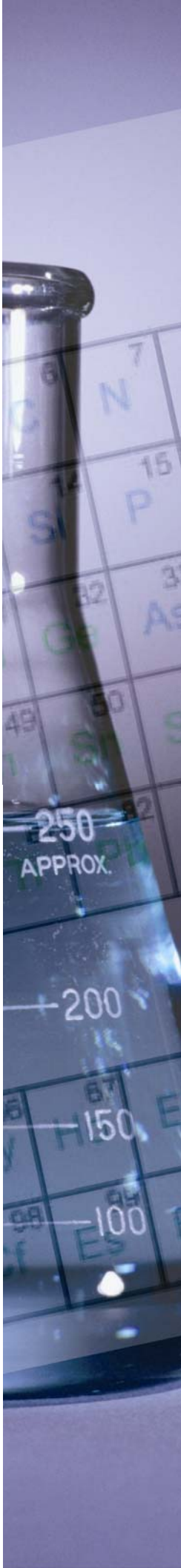
Today's ICS have become an essential element in the management of complex processes and production environments. The risk of exploitation by physical or cyber means with the intent to cause harm is real and can have negative impacts on an asset owner's business, public safety, the environment, and national security. Asset owners within the Nation's critical infrastructure 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

critical infrastructure 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 ICS cybersecurity has been increasing over the past several years. Based on previous efforts in the Energy and Water Sectors, five general 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. They are also constructed in a classic problem-solving pattern: identify the problem, establish a problem solving methodology, solve the problem, and evaluate the problem in the future to ensure continuing fixes as needs arise. The first three goals are technical, the fourth encompasses programmatic, management, and cultural achievements, and the fifth encourages and facilitates a partnership between asset owners and ICS vendors to make security an integral part of the specified and produced systems. The following list briefly describes each goal:

- ***Measure and assess security posture*.** Companies will have a thorough understanding of their current security posture to determine where ICS vulnerabilities exist and what actions may be required to address them. Within 10 years, the sector will help ensure that asset owners have the ability and commitment to perform fully automated security state monitoring of their control system networks with real-time remediation.
- ***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 for legacy systems, but 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 ICS components and architectures that offer built-in, end-to-end security. This replacement will not typically be driven solely by security related concerns.
- ***Detect intrusion and implement response strategies*.** Cyber intrusion tools are becoming sophisticated to the degree that any system can become vulnerable to emerging threats. Within 10 years, the capability will exist for Chemical Sector operating networks to automatically provide contingency and remedial actions in response to attempted intrusions.
- ***Sustain security improvements*.** Maintaining aggressive and proactive cybersecurity of ICS 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, Chemical Sector asset 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 ICS.
- ***Secure-by-design*.** ICS products will be secure-by-design within 10 years. Chemical Sector owners and operators will insist, through specifications and orders, that vendors provide systems that are secure-by-design, and will work with vendors to achieve this goal.

These goals provide a logical framework for organizing the collective efforts of industry, government, and other key stakeholders to achieve the vision. To be successful, however, specific milestones and deliverables must be accomplished in the 2009–2017 period. Projects,



activities, and initiatives resulting from this roadmap generate the milestones presented and described in Section 3.

CHEMICAL SECTOR PERSPECTIVES

This section addresses issues specific to the Chemical Sector that have an impact on potential security solutions.

BACKGROUND

The NIPP requires each sector to issue a sector-specific plan. As the SSA for the Chemical Sector, DHS worked with the Chemical Sector to prepare the Chemical SSP and its 2008 update.[8]

According to the 2008 update, the Chemical Sector, which includes business valued at $664 billion, can be divided into five segments: basic chemistry, specialty chemicals, agricultural chemicals, pharmaceuticals, and consumer products. The Chemical Sector is very diverse. It includes manufacturing plants, transport systems, and distribution systems that encompass storage, stockpile, supply areas, farm suppliers, and wholesalers.

The Chemical Sector has 863,000 employees and produced $664 billion—21 percent of the total world output in 2007.[9] It is an integral component of the U.S. economy, converting various raw materials into more than 70,000 diverse products, many of which are critical to the health and well-being of the Nation's citizenry, security, and economy. Many of the Chemical Sector industries are also international with international suppliers, manufacturers, and customers. These diverse operations lead to the unique set of risks addressed in this roadmap.

Chemical Sector Facts

- Valued at $664 billion
- 863,000 employees
- 70,000 diverse products
- International network of suppliers, manufacturers, and customers

SECTOR REGULATIONS

In late 2006, Congress passed the *Department of Homeland Security Appropriations Act of 2007*.[10] In addition to providing money for DHS, the law gives DHS the authority to regulate the Nation's highest risk chemical facilities and directs DHS to develop chemical facility security regulations. In response, DHS published the applicable regulations: *Chemical Facility Anti-Terrorism Standards* (CFATS) on April 9, 2007.[11]

The table in Appendix A of the CFATS document, which identifies chemicals of interest and threshold quantities that define a "high risk" facility, was released June 8, 2007. High risk facilities are required to complete security vulnerability assessments and develop site security plans to assess risk and implement protective measures. CFATS includes Risk Based Performance Standards, such as the yet to be issued Risk Based Performance Standards 8 (RBPS-8), "Cyber," which will address cybersecurity as a performance standard. Although working towards implementation of this roadmap is voluntary, it does align with the methodology of RBPS-8.

Chemical facilities with marine ports that are regulated by the *Coast Guard Marine Transportation Security Act*[12] may be exempt from CFATS as described in the authorizing language.

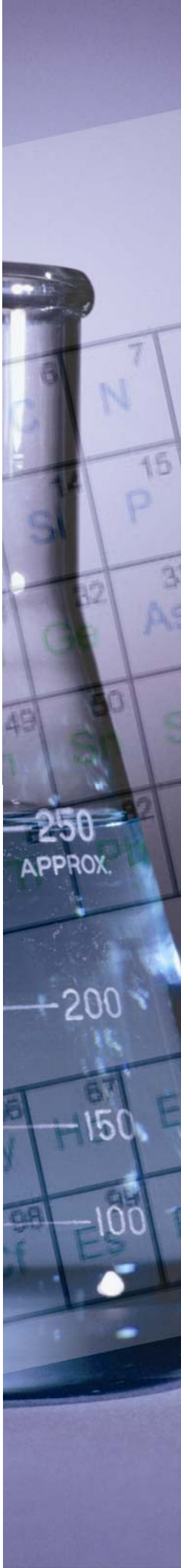
CHEMICAL SECTOR CYBER SECURITY STANDARDS AND PRACTICES

The Chemical Sector has been a leader in developing methods and processes to address safety and reduce risk. The Chemical Sector has long recognized its vulnerability to cyber attack and cybersecurity as an important aspect of risk reduction. The sector has been engaged in understanding the protection of information and assets. Industry activities have included development of guides and standards to assist in improving operational safety and reliability.

The Chemical Sector relies on many different stakeholders including designers, vendors, consultants, systems integrators, suppliers, and market research companies to assist the owner/operators in achieving ICS. The Chemical Sector has been working with several organizations, specifically the Chemical Information Technology Center (ChemITC®), the International Society for Automation (ISA), and the Process Control Security Requirements Forum (PCSRF) to enhance cybersecurity standards and practices. In addition to the stakeholders providing direct support in their primary capacity, they participate in developing the guides and standards by becoming members of these organizations.

CHEMICAL INFORMATION TECHNOLOGY CENTER

In 2002, while the National Strategies[13] [14]on CIKR were being prepared, the U.S. Government sought support from the Chemical Sector to enhance the cybersecurity posture of this critical infrastructure sector. In response, six companies established the Chemical Sector Cyber Security Program (CSCSP) to focus on risk management and reduce the potential for impact due to cyber attacks on business and manufacturing systems. The program quickly expanded to include a number of the larger chemical companies. The CSCSP developed and openly published numerous guidance documents to assist Chemical Sector companies to address their cybersecurity management programs. The guidance initially developed by the CSCSP was incorporated into the Responsible Care Security Code® of the American Chemistry Council (ACC).



The CSCSP is now a program of the ChemITC® that is set up under the ACC. There are 31 ACC member companies participating in the ChemITC®. This represents about 23 percent of the member companies of the ACC and a small percentage of the number of companies within Chemical Sector.

ChemITC® is actively working to address the cybersecurity needs of its member companies and the Chemical Sector. The organization develops and publishes documents addressing cybersecurity issues and relevant guidance to address the issues. All guidance documents are published on the ChemITC® Web site and are accessible to other companies and the public.

In 2006, ChemITC® developed a Chemical Sector Cyber Security Strategy[15] that lists five strategic elements:

1. Share Information;
2. Guidance Enhancement;
3. Sector-wide Adoption;
4. Technological Solutions; and
5. Government Relations.

In support of the strategy items listed above, ChemITC® is actively engaged with the SCC, GCC, ICSJWG, CSCSWG, and other industry-wide security initiatives including the ISA, Institute for Information Infrastructure Protection (I3P), and the PCSRF.

The Chemical Sector Roadmap Working Group recognizes the importance of above strategic elements as key in enhancing control system security throughout the sector. As such, the Chemical Sector Roadmap Working Group has incorporated them into the basis of the goals, milestones, and priorities presented in Chapter 3 of this Roadmap.

International Society of Automation

ISA is a leading, global, nonprofit organization that is setting the standard for automation by helping over 30,000 worldwide members and other professionals solve difficult technical problems while enhancing their leadership and personal career capabilities. ISA has been working to develop cybersecurity standards via the ISA-99 committee on industrial automation and control systems security. This committee has produced several technical reports and standards, with more planned.[5] Members of the Chemical Sector are encouraged to participate in ISA cybersecurity activities.

Process Control Security Requirements Forum

The PCSRF provides another venue for the Chemical Sector to share information with the government and other sectors.

The National Institute of Standards and Technology (NIST), which is working to improve the IT security of networked digital control systems used in industrial applications, created the PCSRF to address security requirements of process control systems. The forum has more than 600 members from government, academia, and private sectors, representing critical infrastructures and related process industries including oil and gas, water, electric power, chemicals, pharmaceuticals, metals and mining, and pulp and paper. Led by NIST, the PCSRF is a working group of users, vendors, and integrators in the process control industry

aiming to present a cohesive, cross-industry baseline set of security requirements for new ICS.

Members of Chemical Sector are encouraged to join and participate in PCSRF.

GOVERNMENT CYBER SECURITY COORDINATION AND SUPPORT

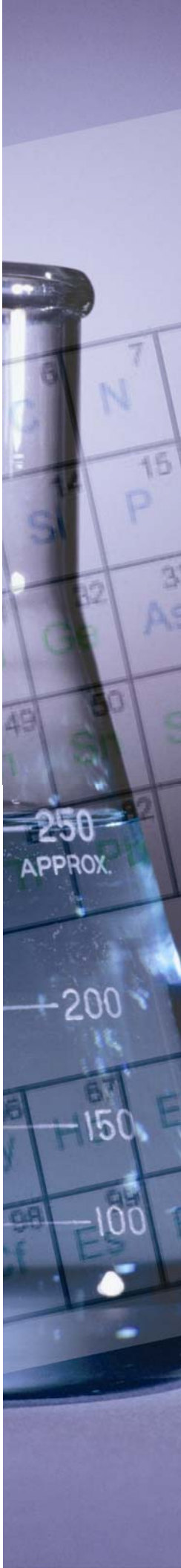
The NIPP relies on the sector partnership framework as the primary organizational structure for coordinating CIKR efforts and activities. As part of this, the government has established SCCs and GCCs. The CSCSWG and the ICSJWG provide further coordination on cyber specific issues. The US-CERT and ICS-CERT are DHS organizations that provide cybersecurity information along with the state organization—Multi-State Information Sharing and Analysis Center (MS-ISAC).

SECTOR COORDINATING COUNCILS

The NIPP sector partnership model encouraged the formation of SCCs. The Chemical SCC is organized and provides a working interface between industry and Federal, State, local, tribal, and territorial partners.

The Chemical SCC currently consists of the following 17 chemical industry trade associations representing diversity in their suite of products, methods of production, and approaches to control, which are committed to enhancing the physical, human, and cybersecurity of the Chemical Sector:

- American Petroleum Institute;
- Agricultural Retailers Association;
- American Chemistry Council;
- America Forest & Paper Association;
- Chemical Producers & Distributors Association;
- Compressed Gas Association;
- CropLife America;
- Independent Liquid Terminals Association;
- Institute of Makers of Explosives;
- International Institute of Ammonia Refrigeration;
- National Association of Chemical Distributors;
- National Paint & Coatings Association;
- National Petrochemical and Refiners Association;
- Society of Chemical Manufacturers and Affiliates;
- The Chlorine Institute, Inc.;
- The Fertilizer Institute; and
- The Society of the Plastics Industry, Inc.



CHEMICAL GOVERNMENT COORDINATING COUNCIL

The Chemical GCC is the Federal counterpart to the Chemical SCC. The Chemical SSA sits as the chair of the Chemical GCC, with responsibility for ensuring appropriate representation on the GCC and providing cross-sector coordination with State, local, tribal, and territorial governments. Members of the GCC include:

- Department of Homeland Security;
- State, Local, Tribal, and Territorial Government Coordinating Council;
- Department of Commerce;
- Department of Defense;
- Department of Energy;
- Department of Justice;
- Department of State;
- Department of Transportation;
- Director of National Intelligence; and
- Environmental Protection Agency; and
- Federal Bureau of Investigation.

The SCC and GCC meet together annually for industry-government coordination. Prior to the development of the SCC, the Chemical Sector had a long history of working with the government to improve its knowledge and understanding of how chemicals interact with human health and the environment. In addition to the work that is done through the SCC with DHS, the Chemical Sector works closely with the FBI, U.S. Department of Defense, U.S. Environmental Protection Agency (EPA), U.S. Department of Transportation, U.S. Department of Energy (DOE), and many others to bring the Federal government's security expertise together with industry innovation.

CROSS SECTOR CYBER SECURITY WORKING GROUP

Like the SCC and GCC, the CSCSWG was established under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC) to allow for government and private sector collaboration. This working group serves as a forum to bring the government and the private sector together to address cybersecurity risk across the CIKR sectors. This cross-sector perspective facilitates the sharing of viewpoints and knowledge about various cybersecurity concerns, such as common vulnerabilities and protective measures, and leverages functional cyber expertise in a comprehensive forum. Managing cyber risk and securing cyberspace is an issue that cuts across the Nation's CIKR, and the cross-sector perspective ensures effective coordination with all of the sectors. The Chemical Sector actively participates in the CSCSWG along with the SCC and GCC.

INDUSTRIAL CONTROL SYSTEM JOINT WORKING GROUP

The DHS Office of Cyber Security and Communications established the ICSJWG as a recognized CIPAC organization in December 2008. The ICSJWG is a collaborative coordination body operating under CIPAC. It was established to facilitate the collaboration of

control systems stakeholders and to accelerate the design, development, and deployment of enhanced security for control systems. ICSJWG participants include international stakeholders, government, academia, owner/operators, systems integrators, and the ICS vendor community. Although its objective is to reduce the risk of cyber control systems, which is the same as that of this roadmap, the ICSJWG scope is coordination across all CIKR Sectors, whereas this roadmap's focus is within the Chemical Sector.[16]

United States Computer Emergency Readiness Team

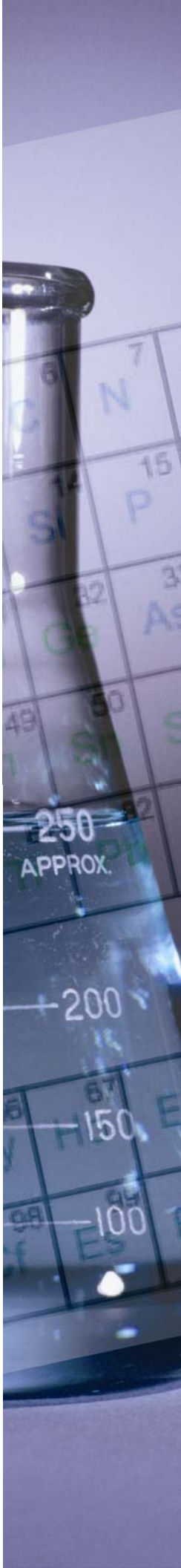
The US-CERT is a partnership between DHS and the public and private sectors. Established in 2003 to protect the Nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the Nation. A special section is devoted to control system security.[17]

Industrial Control System – Cyber Emergency Response Team

The ICS-CERT operates as a functional element of the US-CERT for cyber incidents related to ICS. The ICS-CERT is responsible for analyzing and responding to cyber threats or issues affecting control systems security in critical infrastructure. DHS has recognized the need to expand upon these technical and response capabilities in order to improve situational awareness and incident response and to mitigate vulnerabilities. This expansion encourages government and the private sector participation by reporting and sharing incident and vulnerability information.[18]

Multi-State Information Sharing and Analysis Center

The MS-ISAC[19] is a collaborative organization with participation from the 50 States, the District of Columbia, local governments, and the five U.S. Territories. The mission of the MS-ISAC is to provide a common mechanism for raising the level of cybersecurity readiness and response in each State and with local governments and the territories. It provides a central resource for gathering information from the states on cyber threats to critical infrastructure and providing two-way sharing of information between and among the states and with local government.



3. CHALLENGES, PRIORITIES, AND MILESTONES

This section addresses the challenges facing control system security, the selected priorities for action, and the goals that will 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

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 those factors that limit the ability to implement ideal security enhancements.

Risk is defined by threat, vulnerability, and consequences. 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 degree of hazard of the material; the value of the material and systems; and how loss of control can lead to interaction with humans, property, and the environment.

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

Challenges related to the implementation of security measures include organizational, institutional, economic, and technical factors that either limit the availability of security measures, 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. This roadmap includes the challenges identified in the *Energy Sector Roadmap*, but adds others that evolved after the *Energy Sector Roadmap* was issued and those specific to the Chemical Sector.

The following references were searched for problem statements, issues, and challenges to securing the ICS used in CIKR.

- CERT Focus Paper (2005)[20]
- ChemITC's Chemical Sector Cyber Strategy[21]
- Chemical Sector Roadmap Development Team
- Chemical Sector Roadmap Team Kickoff Meeting
- Control Engineering article (2007)[22]
- DHS CSSP, program experience including site assessments
- GAO reports 04-354 and 07-1036[23,24]

- ISA Cyber Policy Recommendations (2008).[25]

Based on this search, lists of challenges and issues were generated and analyzed to establish a basis for suggesting the actions and milestones needed to achieve the goals and vision of the Chemical Sector. This search resulted in over 200 separate but not necessarily unique challenges and issues, which are listed in separate tables in Appendix B. The challenges were analyzed and placed in 11 categories: system vulnerability, accessibility, international, risk analysis, business case, design, implementation, standards, training, information sharing, and coordination.

Table 1 correlates these 11 categories with the five goals.

Table 1. Cross-Walk Between Goals and Challenges

Goals	Meet Challenges
Measure and assess security posture	• System vulnerability • Implementation • Risk Analysis • Business case
Develop and integrate protective measures	• System vulnerability • Design • Implementation • Standards
Detect intrusion and implement response strategies	• Accessibility • Implementation • Information sharing
Sustain security improvements	• Business case • Coordination • Design • Information sharing • International • Risk Analysis • Standards • Training
Secure-by-design	• Design • International • Standards

One key technical challenge is the issue of accessibility, both physical and cyber, which could enable an attacker to take advantage of known and yet-to-be-discovered vulnerabilities. The accessibility issue is exacerbated by the nature of the Internet and global interdependencies of CIKR: an attack could originate from almost anywhere on the planet; CIKR companies often have international partners, suppliers, and customers; and cyber components and systems often have international origins with international maintenance and support.

Risk assessment and analysis will provide an analytical understanding of this problem. The business case is a subset of risk analysis in that it provides an understanding of the cost benefit of expending resources to reduce risk. Once the problem is recognized and understood through assessment and analysis, it will be possible to design and implement solutions that will act as countermeasures to the system vulnerabilities. Security systems and procedures

should be designed and implemented in accordance with industry standards and accepted practices. Training enables all stakeholders to take proper actions.

Continuous improvements will be driven by information sharing and coordination supporting the identification and development of efficient solutions in an environment consisting of many governing and regulatory agencies, thousands of independent facilities, and hundreds of vendors and R&D organizations. Ultimately, this roadmap seeks secure-by-design solutions that address technological and international challenges.

PRIORITIES FOR SECURING CONTROL SYSTEMS

From the list of challenges, several priorities were identified based on the potential to affect the greatest change and the need for immediate improvements. Priorities often begin as a simple reversal of the challenge. For example, the challenge—*Practical and cost-efficient assessment tools are needed, but not widely available,* leads to the priority—*Fund efforts to develop a tool set for owners and operators to conduct self assessments*.

The tabular development of issues and challenges is presented in Appendix B. The subsequent priorities needed to resolve those issues and challenges are presented in Appendix C.

MILESTONES

The priorities formed the basis for selecting milestones. The milestones were selected, discussed in detail, modified, and finalized during the development of this document with members of the Chemical Sector Roadmap Working Group. The development of these milestones, along with comments and a comparison to the milestones in the Energy Sector Roadmap, is detailed in Appendix D.

A brief summary of milestone development followed by a graphical depiction of the challenges, priorities, and milestones for each goal are presented below.

GOAL 1: MEASURE AND ASSESS SECURITY POSTURE

Goal 1 requires the use of methodologies, training, standards, and accepted industry practices to understand the systems at risk and the factors that contribute to risk. The complexity of cyber control systems requires automated tools. Measurement of security requires the existence of agreed upon metrics. All of these requirements have been previously explored, and the knowledge base is rapidly increasing.

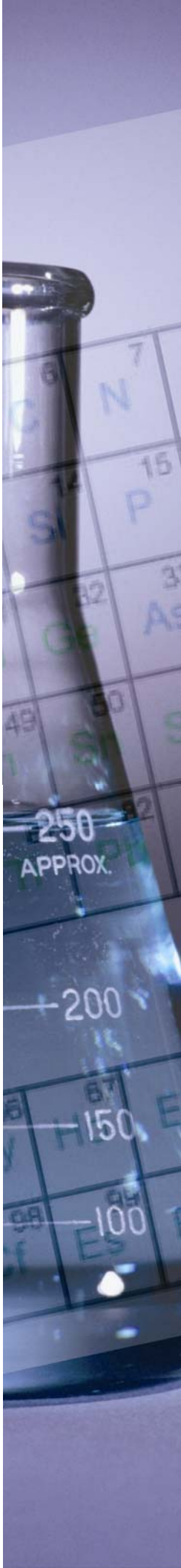
Communicating the information related to ICS cybersecurity threats, vulnerabilities, and risks requires the availability of industry accepted practices, tools, and training materials, which became partially available at the end of 2008. Mechanisms are in place to communicate new information related to the first milestone. DHS has developed self-assessment tools,[26] which are available for use by chemical sector asset owners and operators. The CSSP is working with critical infrastructure stakeholders to encourage the practice of conducting ICS security self-assessments using these tools. The vision is to reach a point where most facilities would also have fully automated real-time security state monitors to assess their security posture in real time.

GOAL 2: DEVELOP AND INTEGRATE PROTECTIVE MEASURES

Goal 2 requires the implementation of the training, tools, and methods necessary to secure ICS. Training courses have been developed and are now being offered to asset owners to help increase awareness and change the culture of security practices related to ICS.

As the understanding of the vulnerabilities resulting from interfaces between businesses and ICS becomes common knowledge, those interfaces will be secured. The recent 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.

Periodic non-disruptive testing of ICS is required to verify that the systems, as designed, installed, and maintained, are effective in detecting, isolating, and automatically responding to cyber attacks. The long-term vision is to move towards installing cyber resilient ICS architectures that have built-in security and use systems and components that are secure-by-design.



Goal 1
Measure and Assess Security Posture

Challenges

1. A cyber attack on a vulnerable ICS could result in business interruption, loss of capital, and impacts to plant employees, public safety, the environment, and national security
2. Inventory of critical assets, their associated ICSs, and the risk of cyber attack are often not adequately known or understood
3. Practical and cost-efficient assessment tools are needed but not widely available
4. Knowledge and understanding of risk, including threat, vulnerability, defense, and consequence analysis capabilities across the sector is limited
5. Metrics to measure cyber security posture and/or improvements over time and across the sector are needed but not available
6. Security vulnerability assessments are needed to determine the consequences of specific cyber security compromises of ICSs
7. Security metrics are required to perform detailed threat analyses
8. Existing standards lack meaningful and measurable specifications relating to ICS cyber security
9. Cyber security threats are difficult if not impossible to quantify, but quantified values are required for quantified risk estimation
10. Cyber risk factors are neither widely understood nor accepted by technologists and managers
11. Current standards for assessment of cyber vulnerabilities are inadequate
12. Consistent metrics are necessary but not available to measure and assess security status

Milestones

2009

- Establish an industry-driven awareness effort to communicate information relating to the cyber security threats, vulnerabilities, and risks and the availability of recommended practices, tools, and training materials to the Chemical Sector.

2010

- Metrics for benchmarking security posture are available and agreed upon.

2012

- Asset owners and operators are performing self-assessments of their ICSs using consistent criteria.
- Real-time security state monitors for new and legacy systems are in use.

2017

- Fully automated security state methodologies are in use.

Selected Priorities

1. Create a risk matrix that balances threat, vulnerability, and consequence
2. Analyze risk and determine what action is appropriate
3. Continue to enhance and fund efforts to develop a tool set for owners and operators to conduct self assessments
4. Set up and evaluate cyber attack and response simulators
5. Develop consensus on clear and concise metrics for measuring security posture
6. Develop risk assessment tools that include vulnerability assessment methodologies, frameworks for prioritizing control measures, and cost justification tools
7. Develop baseline security requirements defined across system life cycles for fundamental, intermediate, and advanced security posture
8. Develop automated security state and response support systems
9. Create an environment for securely sharing collected U.S. Government information on threats and real-world attacks with utilites and vendors
10. Encourage participation with HSIN-CS

Goal 2
Develop and Integrate Protective Measures

Challenges

1. Widespread and continuous connectivity of IT and ICSs, and generally, with remote access by multiple parties or devices, provides opportunity and routes for cyber attack
2. Many ICSs operate using unauthenticated command and control data
3. Many ICSs have remote access points without appropriate or adequate access control
4. Many ICSs have been designed, built, and operated within open communication environments
5. The unavailability of patch management that conforms to a 24/7 production environment with extended vulnerability windows and without regularly scheduled maintenance opportunities leads to windows of opportunity for cyber attack on systems with known but unfixed vulnerabilities
6. Older operating platform (legacy and hybrid) systems may have limited or no vendor/service support, thus limiting their ability to secure the systems
7. Existing ICSs with numerous access points, default vendor accounts/passwords/shared passwords, and poor firewall implementation provide increased cyber attack opportunities
8. Basic security features are often not enabled
9. The complexity of ICSs increases exponentially with an increase in the number of nodes, thereby increasing attack opportunities
10. Security upgrades are hard to retrofit to legacy ICSs, may be costly, and may degrade system performance, thus lessening incentives to upgrade those systems
11. Risks can arise from using non-vendor hardware and software

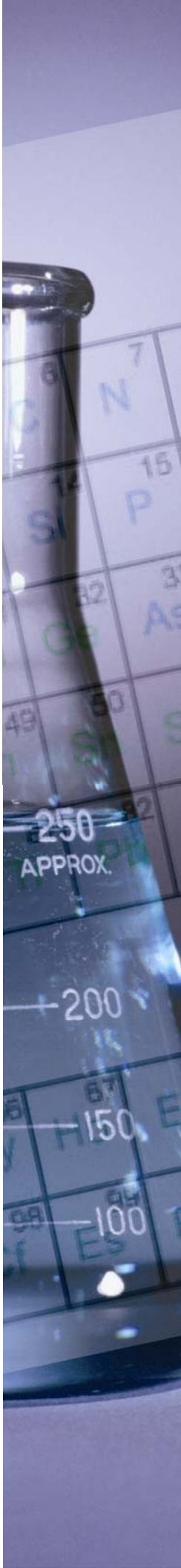
Milestones

2009 — **2010** — **2011** — **2018**

- Sector is participating in security training to available, qualified, and consistent control system security training materials.
- Secure connectivity between business systems and ICSs within corporate networks.
- Perform nondisruptive intrusion tests on ICSs to demonstrate the effectiveness of automated isolation and response.
- Widespread implementation of methods for secure communication between remote access devices and control centers that are scalable and cost effective to deploy.
- Secure ICS architectures with built-in, end-to-end security are in all critical operating systems.

Selected Priorities

1. Identify acceped practices for physical and cyber security of control centers
2. Develop cost-effective gateway security that includes firewalls, intrusion detection, and anti-virus protection with minimum host impact
3. Develop a security test harness with testing architecture and guidelines
4. Work with vendors and asset owners to test equipment, architectures, and processes for both cyber and physical security
5. Develop patching technologies that do not impact 24/7 operations of operating systems
6. Improve performance of legacy communications to enable the application of security solutions
7. Identify best practices for connecting ICSs and business networks
8. Put nonintrusive, cost effective, and robust ICS encryption solutions into production
9. Develop hardened operating systems for the ICS environment



GOAL 3: DETECT INTRUSION AND IMPLEMENT RESPONSE STRATEGIES

Goal 3 requires provisions to detect and respond to those attacks that manage to defeat the protective measures of Goal 2.

The milestones for Goal 3 are, therefore directed towards ICS incident handling, including detection, response, and recovery from an all hazards perspective. Incident reporting is an integral part of security enhancement, which is consistent with generally agreed upon principles that reporting incident information and lessons learned and sharing that information leads to total system improvement. The National Cyber Security Division has established a mechanism (US-CERT: https://forms.us-cert.gov/report/) to report vulnerabilities and incidents and the ICS-CERT to address specific ICS concerns. The largest challenge to voluntary incident reporting is protecting proprietary information; trust has yet to be gained that such information will be protected and not misused.

More automation in both response and recovery is also needed. A direct method of enhancing the response recovery is to incorporate these procedures and processes into well-established emergency operating plans.

GOAL 4: SUSTAIN SECURITY IMPROVEMENTS

Goal 4 will be accomplished through capturing new and necessary information and then sharing that information across the sector. It also includes planning and updating strategies, providing education and awareness training, and developing new methodologies; specifically, the business case. Many people also believe that government incentives could help to ensure that necessary security enhancements are in place, depending on the cost of those enhancements.

Most of the resulting milestones—awareness campaigns, information sharing, collecting and sharing threat and vulnerability information, development of the business case, and security upgrade incentives—will be the responsibility of all stakeholders to address ICS cybersecurity. It is expected that universities, colleges, specialized vendors, companies, and employers will provide programs to train professionals in cyber control system security.

GOAL 5: SECURE-BY-DESIGN

Goal 5 relies primarily on the development of new technologies that are designed, built, and tested to achieve secure operation. Most Goal 5 milestones therefore rely on the ingenuity of the R&D community and the manufacturers of ICS hardware and software. The Chemical Sector owners and operators will participate by specifying secure-by-design when procuring new systems. Owners and operators will also work with vendors to collaborate on improvements to built-in security.

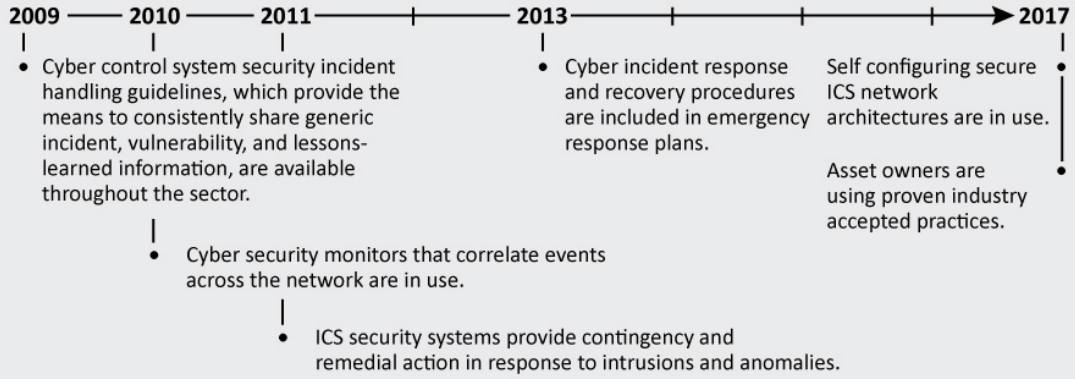
There is a good deal of interest in having an independent certification center to certify the security levels of new and existing systems and components. Several security certification systems are currently on the market. The ISA Security Compliance Institute[27] was established to meet this need, but it is not yet operating. The desired security certification center may well be available before the milestone date of 2018.

Goal 3
Detect Intrusion and Implement Response Strategies

Challenges

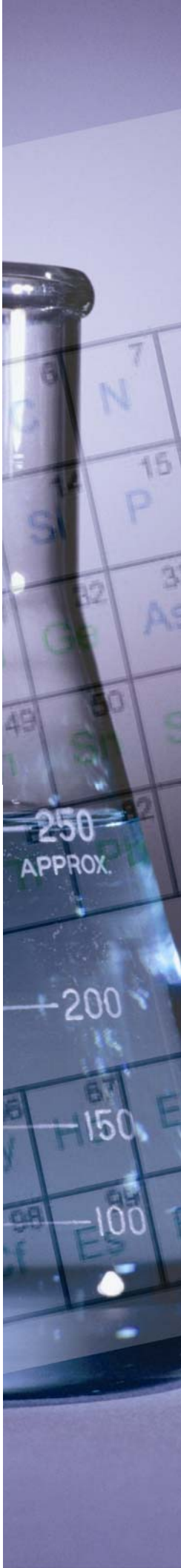
1 Periodic and appropriate reviews of security logs and change management documentation often receive limited if any attention
2 Cyber security measures may negatively impact rapid response to emergencies
3 The continual increase in the sophistication of hackers tools and resources increases attack risk

Milestones



Selected Priorities

1 Develop and deploy sensors and sensor systems with mechanisms to detect and report anomalous activity
2 Develop automated security state and response support systems
3 Identify industry-approved incident reporting guidelines and best practices
4 Expedite security clearances for industry to facilitate information sharing and incident reporting
5 Develop and provide training on incident response procedures and tools
6 Adapt intrusion prevention system for more robust application to networks and hosts
7 Develop tools for security event management
8 Enable automated collection of security information, including incidnt reports and visualization tools for correlation
9 Develop intrusion detection system/intrusion protection sytem products for control systems and audit trails with automated reporting
10 Designate a staff member at each chemical industry facility with responsibility to utilize, maintain, or support cyber control systems as the ICS-CERT/US-CERT contact point



Goal 4
Sustain Security Improvements

Challenges

1 Necessary and constructive relationships with governmental authorities for availability, reliability, and accessibility of threat information for the sector are often lacking
2 Cyber security has too often been handled separately for more traditional company security and safety programs
3 Federal legislation to enhance national cyber security guidelines for chemical facilities that proceeds with limited input from owner/operators will create implementation problems
4 Inadequate policies, procedures, and culture relating to ICS cyber security negatively impacts security and increases risk
5 Chemical facilities often have toxic, flammable, and explosive chemicals that provide attractive targets for terrorists to release, steal, or sabotage
6 Without active input from owner/operators, cost efficient compliance with 6 CFR 27, consistent across the sector, that is adequate and appropriate to the risk-based tier level for each facility, will be difficult to achieve
7 Differing business models and risk profiles within the same operational boundaries (not all parts of a given plant have the same potential for severe consequences) increases the difficulty and incentives to implement cyber security measures
8 Discovery of vulnerabilities, improved awareness, implementation of protective measures, and application of continuous improvement relative to cyber security is necessary to stay ahead of potential cyber attackers
9 Funding and implementation of enhanced security measures is difficult without executive recognition of ICS security threats and liabilities
10 Implementation of cyber-security across the entire sector is difficult due to varying needs of asset owners, and there is a large number of different asset owners
11 Funding of activities (R&D, for example) important to ICS security depends on input from industry to properly align government and industry goals
12 Consistent standards, requirements, and guidance from sector-specific agencies is limited or lacking
13 The Chemical Sector has a significant diversity of processes and products (>70,000 products), which increases both the risk to and the difficulty of enhancing ICS cyber security
14 Dissemination of ICS security information to the large number of asset owners in the Chemical Sector with diverse interests is complicated
15 ICS cyber security across the many types of production facilities within the sector is currently not always based on industry accepted practices
16 Traditionally there has been a collaboration barrier between IT and ICS departments that can lead to inconsistent and redundant security measures
17 Poor coordination among government agencies creates confusion and inefficiencies
18 New regulations may impose requirements beyond the functional capability of legacy systems
19 Limited knowledge, understanding, and appreciation of security risks inhibits constructive, necessary, and sufficient cyber security enhancement and implementation
20 A cyber security business case based on enhanced risk analyses, which could quantify and prioritize necessary and sufficient security measures and justify the costs, is required but not available
21 Effective security-oriented partnerships between government and industry have been difficult to establish
22 Asset owners fear the loss of intellectual property rights by widely and openly sharing incident and assessment information related to enhanced ICS security measures
23 Inadequate and insufficient sharing of cyber threat and incident information between government and industry negatively impacts the ability to properly assess risk and select appropriate cyber security measures

Goal 4
Sustain Security Improvements

Milestones

2009

- Create secure forum for sharing cyber threat and incident response information throughout the Chemical Sector.
- Ensure that progress on security improvement efforts presented in this roadmap is periodically shared with the Chemical Sector.

2010

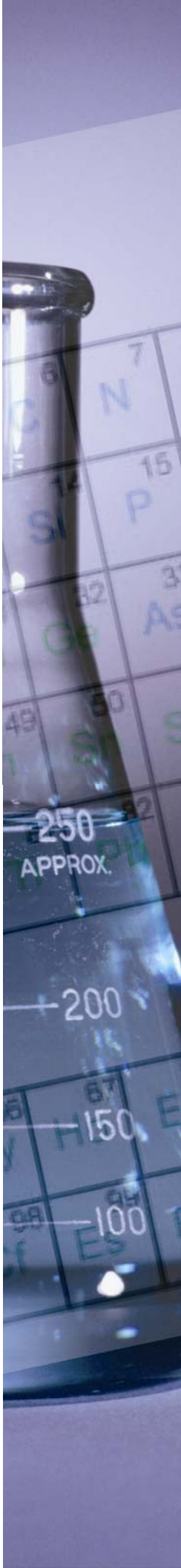
- Develop compelling evidence-based business case to explain the cost-efficient investement in control system security.
- Integrate cyber security awareness, education, and outreach programs into the Chemical Sector.
- Undergraduate curricula are available at academic institutions in control systems security; scholarships, internships, and research grants are also available.

2011

- Obtain meaningful incentives through federal and state government to accelaerate investment in secure control system technologies and practices.

Selected Priorities

1 Develop standards and/or regulations for secure data exchange and communications
2 Conduct analysis of incentives and benefits of implementing security to help fortify the business case
3 Create appropriate incentives to invest in control systems security
4 Create a cost-shared control systems security consortium that is protected from anti-trust issues
5 Develop and implement security training for all employees and contractors
6 Develop curricula and university programs to improve education and control systems, security and risks, and associated economics
7 Facilitate information sharing by guaranteeing protection of industry critical infrastructure protection information through legislation or other means
8 Encourage participation in supported industry activities
9 Direct official interaction with the DHS through the Chemical Sector Coordinating Council security activities, particularly ISA99 Industrial Automation and Control Systems Security
10 Work with the government to develop cyber risk methodologies consistent with the needs and interests of the Chemical Sector
11 Host two sector-specific cyber security networking meetings each year
12 Periodically review and assess existing guidance documents to evaluate their relevancy under current conditions and incorporate emerging needs and potential enhancements



Goal 5
Secure-by-Design

Challenges

1. The increasing use of standardized ICSs increases attack opportunity
2. Enhanced cyber security upgrades on ICSs with long design lives that were not initially designed for current cyber security requirements may be difficult and not obviously cost efficient
3. Security that is not necessarily integrated into a vendor's ICS products increases inherent vulnerabilities, requires retrofits and upgrades, and still results in a less secure system
4. Poorly designed interconnections between ICSs and business networks can dramatically increase vulnerabilities and attack opportunities
5. Standardized security test plans and upgrades for all new-technology systems and components are not, widely, available, if at all
6. Tools and techniques sufficient to quantify or measure risk do not exist
7. Vendors do not have adequate requirements or standards to design and build cyber security into ICSs.
8. Tested and validated cyber security tools for ICSs are lacking

Milestones

2009

- Commercial products are available that correlate events across the network.
- Owner/operators collaborate with vendors on system and component security improvements.

2010

- Owner/operators specify secure-by-design when procuring new cyber ICSs.

2011

- Real-time security state monitors for new and legacy systems are commercially available.

2015

- Features are available that provide for fully automated security state and common response ICS networks.
- Secure ICS architectures are designed, installed, and maintained with built-in, end-to-end security.
- All COTS (commercial-off-the-shelf) cyber ICSs and stand-alone components are secure-by-design.

2016

- A certification center with the capability to verify that cyber ICSs and components are secure is available.

Selected Priorities

1. Develop true plug-and-play components that are secure
2. Strive for ICS products that are secure-by-design
3. Specify systems, that are secure-by-design when procuring or upgrading new systems
4. Work with vendors where possible to assist in achieving the secure-by-design goal
5. Increase automation in the technical implementation of cyber security policies, procedures, and practices
6. Establish a certification center with the initial capability to demonstrate that cyber control systems and components meet established security standards and evolve to a capability to demonstrate systems and components secure-by-design

4. ROADMAP IMPLEMENTATION

This roadmap contains a structured set of priorities that address specific ICS needs over the next 10 years. The Chemical Sector will pursue a focused, coordinated approach that aligns current activities to roadmap goals and milestones, initiates specific projects to address critical gaps, and provides a mechanism for collaboration, project management, oversight, and information sharing among the sector stakeholders. The objective of this coordinated approach is to accomplish clearly defined activities, projects, and initiatives that contain time-based deliverables tied to roadmap goals and milestones.

A Chemical Sector Roadmap Implementation Committee is proposed to obtain industry feedback and commitment to participate in needed activities through outreach and partnerships. The Chemical SCC provides an established body that represents asset owners and operators of the Chemical Sector. The SCC also includes association representatives and facilitates physical and cybersecurity efforts within the sector and with government agencies. To ensure its formal recognition, the Chemical Sector Roadmap Implementation Committee will operate under the direction of the Chemical SCC.

Periodic regional roadmap implementation workshops organized by the Chemical Sector Roadmap Implementation Committee should be held to inform the sector of goals and milestones, provide awareness training, and solicit new ideas for the activities directed towards meeting the milestones defined in Section 3. Government agencies should consider aligning resources and funding of priorities based on the elements outline within the roadmap. These priorities often focus on long-term needs or efforts, which limit incentive for business investment. It is recommended that DHS CSSP coordinate with the Chemical SCC in providing subject matter expertise for these workshops.

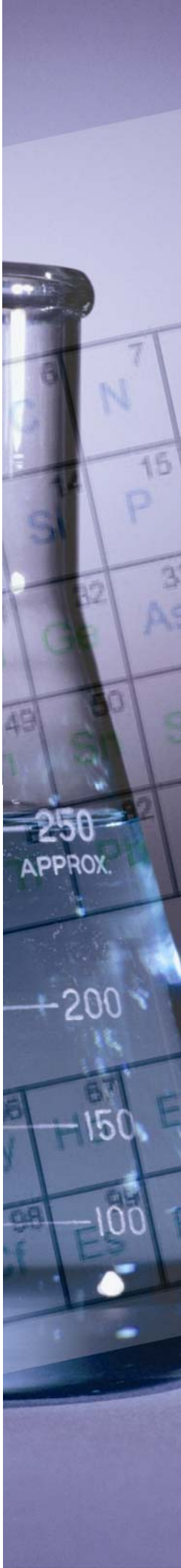
Asset owners and operators are responsible for the security of their facilities and, therefore, must initiate business-critical projects that will ensure reliable, secure operation of chemical facilities and assets. If asset owners and operators demand secure, reliable, and cost efficient systems and components, vendors will be incentivized to meet customer requirements.

PRIMARY IMPLEMENTATION CHALLENGE

The security enhancement elements laid out by this roadmap are voluntary. They specifically avoid calling for regulation that would impose these priorities and actions on owner/operators and vendors.

Since the inception of DHS CSSP, it was envisioned that ICS security enhancements would be incorporated into the production cycle based on each organizations understanding of the cost benefit of implementing security enhancements to reduce the risk of attack. This economic justification, or the cost-benefit analysis, is known as the business case described in Milestone 4.4.

The difficulty in developing the business case arises from the evolutionary nature of cyber systems and the fact that there is no long-term experience to project valid attack rate estimates. Quantifying the types of significant critical infrastructure attacks is also a challenge since 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 were selected to enhance understanding of the need for system evaluations and risk assessments and analyses and could ultimately result in a reliable business case that would resolve the challenge, i.e., justify voluntary investment in necessary cybersecurity enhancement.

The challenge is to find a way to implement a voluntary effort 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 ICS vendors.

PROPOSED MECHANISM FOR OVERSIGHT AND PROJECT MANAGEMENT

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

MANAGEMENT

A Roadmap Implementation Committee, consisting of members from key stakeholder groups, organizations, and government agencies, will be established to coordinate, identify, track, and resolve roadmap implementation issues. The committee will interface with stakeholders to resolve technical concerns, provide transition guidance, assist organizations that have program management issues, and act as a monitor and central clearinghouse for the actions and milestones discussed in this roadmap. The committee may also assist in the review of proposals (subject matter review), provide recommendations on proposed work efforts, provide support, and develop future implementation strategies, as requested.

To support the Chemical Sector roadmap, government and industry resources will be required to sponsor the maintenance of a website. Committee members within the Chemical Sector, government, R&D organizations, academia, and vendor community, similar to the Chemical Sector Roadmap Working Group, are needed to support additional voluntary activities. In order to implement the voluntary goals of this roadmap, the chemical SCC will assist (if requested) in providing project manager subject matter expertise. The private sector project manager will report to the Chemical SCC and work with the DHS CSSP by leveraging existing products and services. The project manager may request the assistance of volunteers within the Chemical Sector on specific activities related to monitoring, surveying, benchmarking, and tracking the progress of this roadmap.

STRUCTURE AND WORKFLOW

The Roadmap Implementation Committee will support roadmap projects and cybersecurity initiatives being promoted or tracked by the Chemical SCC. A schedule for periodic reviews and reporting of roadmap progress will ensure accountability and information sharing with sector membership. This support will include electronically publishing and tracking deliverables and outcomes of projects, providing feedback, and the electronic posting of information sharing and awareness topics addressed in the roadmap milestones that are not otherwise provided for in related information sharing outlets. The committee will hold, host,

support, and/or organize periodic meetings that bring interested parties together 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 Chemical SCC and requests will be sent to the stakeholders stating the problem and seeking their support. This support may include 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 rollout, training/outreach, or any other means or method that advances a particular milestone.

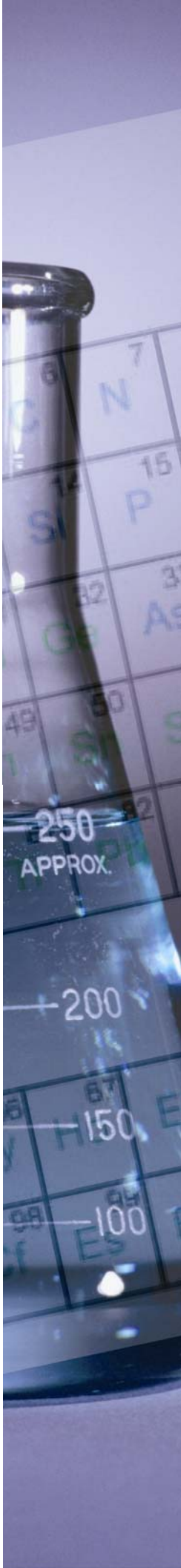
OPERATIONAL OVERSIGHT

Logistical assistance will be required to support meetings, including the provision of adequate meeting space, facilitation, and workshops that will provide needed continuity for roadmap efforts. Allowance should be made for collaboration tools, such as separate electronic space, teleconference meetings, and web-based meetings.

ROLES AND RESPONSIBILITIES

Some of the primary roles and responsibilities of the various sector security partners with regard to the coordination, refinement, and execution of the overarching Chemical Sector protective program are listed in this section. The following list of responsibilities is not necessarily associated with particular programs, projects, or funding and does not constitute a commitment by a specific company, organization, or government agency:

- Roadmap Implementation Committee:
  - Coordinate, identify, track, and resolve roadmap implementation issues
  - Monitor, survey, and track the progress of this roadmap
  - Provide an interface among stakeholders to resolve technical and program management roadmap implementation issues
  - Function as a monitor and central clearinghouse for the actions and milestones discussed in this roadmap.
- DHS:
  - Identify CIKR protection priorities for the Chemical Sector
  - Provide information to help inform protective program decisions
  - Manage and facilitate the ICSJWG to coordinate deployment of Federal resources and minimize duplication of efforts
  - Support Federal, State, local, tribal, territorial, and private sector efforts by sharing threat information and issuing warnings.
- Non-DHS Federal entities:
  - Provide information to help make 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 with additional knowledge from the state/local level 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 owner/operators:
  - Interact with DHS (US-CERT and ICS-CERT) to leverage available threat, incident, and vulnerability information
  - Implement site-specific protective measures
  - Participate in identifying accepted industry practices
  - Report ICS, cyber incidents, or newly discovered vulnerabilities to the US-CERT at *http://www.us-cert.gov/control_systems/*
  - Share information within the Chemical Sector and Federal agencies as required.

- Universities and colleges:
  - Develop cyber ICS security courses.
  - Establish cyber ICS security degree programs
  - Support the establishment and awarding of scholarships, fellowships, research assistantships, and other student financial support mechanisms.

GUIDING AND ALIGNING EXISTING EFFORTS

As discussed in Section 2 and summarized in Table 3, a significant effort to enhance ICS 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 3. 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 ICS	• ICSJWG quarterly and annual meetings.
Process Control Security Requirements Forum (PCSRF)	National Institute of Standards and Technology	Industrial process control systems security requirements	• *System Protection Profile for Industrial Control Systems (SPP-ICS)*, Version 1.0 released (2004)
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
Chemical Information Technology Center (ChemITC)	American Chemistry Council (ACC)	Address common IT issues and support the industry's ability to safely and efficiently deliver products essential to society	• R&D • Industry accepted practices • Outreach, awareness, and information sharing • Partnership development • Vulnerabilities disclosure • Threat information • Business continuity
National Petrochemical & Refiners Association (NPRA)	A national trade organization	Represents U.S. refiners and petrochemical manufacturers in areas of safety, government relationships, and policies affecting the industry	• Cyber Security Subcommittee provides information and recommendations to the NPRA members on matters pertaining to cybersecurity and cyber terrorism targeting business systems and/or control systems in the refining and petrochemical industries
American Gas Association (AGA) 12 Guidance	AGA, Gas Technology Institute (GTI), and NIST	Cryptographic guidelines for SCADA communication	• AGA 12, Parts 1 and 2 Working Guidelines released (2003–2005) • AGA 12, Parts 3 and 4 under development
America Petroleum Institute (API)	Trade association for the oil and natural gas industry	Industry forum, research center, and policy input	• API Standard 1164, *Pipeline SCADA Security* (2004) • Other security guidelines under development

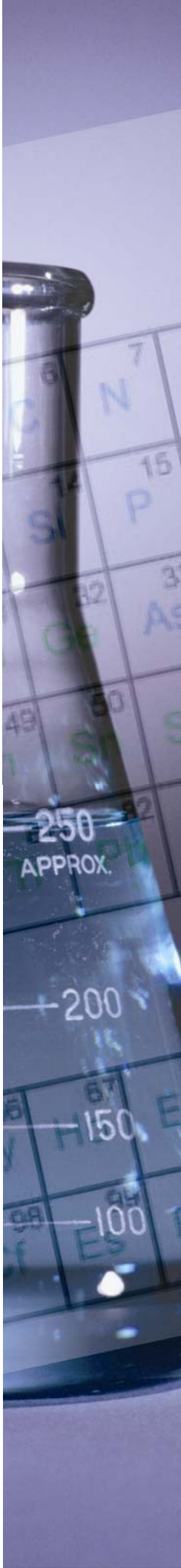
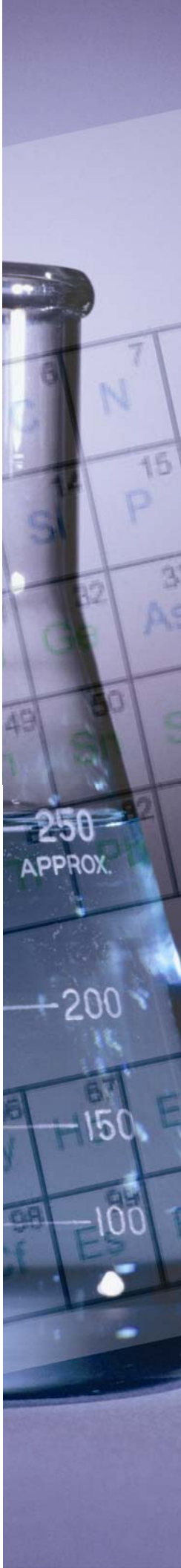


Table 3. (continued)

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 EXPO (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 Operational – Planned May 2009
CFATS	IP	Covered facilities	• Risk Based Performance Standard 8

5. REFERENCES

1. *Roadmap to Secure Control Systems in the Energy Sector*, Sponsored by DHS and DOE, January 2006.
2. Water (WSCC) Cyber Security Working Group (CSWG), *Roadmap to Secure Control Systems in the Water Sector*, Sponsored by DHS and the American Water Works Association, March 2008.
3. Department of Homeland Security, *National Infrastructure Protection Plan*, 2006.
4. Bush, President George W., 2003, *Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection*, Washington, D.C., www.whitehouse.gov/news/releases/2003/12/20031217-5.html.
5. ISA-99 Standard, ANSI/ISA-99.00.01-2007: *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models.*
6. GAO 08-113, *Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*, October 2007.
7. Special Publication 800-82, FINAL PUBLIC DRAFT, Keith Stouffer, Joe Falco, Karen Scarfone, September 2008, http://csrc.nist.gov/publications/PubsSPs.html.
8. Department of Homeland Security, *Chemical Sector-Specific Plan*, Annual Update to the Chemical Sector-Specific Plan, May 2008.
9. *Guide to the Business of Chemistry 2008*, American Chemistry Council.
10. *Department of Homeland Security Appropriations Act of 2007*, H.R. 5441, 109th Congress. October 4, 2006
11. 6 CFR § 27, "Chemical Facility Anti-Terrorism Standards (CFATS)," *Code of Federal Regulations*, April 9, 2007.
12. *Coast Guard Marine Transportation Security Act*, Public Law 107–295, 107th Congress, November 25, 2002.
13. *The National Strategy to Secure Cyberspace*, February 2003, http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.
14. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003, http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.
15. Chemical Sector Cyber Security Program Steering Team, *U.S. Chemical Sector Cyber Security Strategy*, American Chemistry Council, September 2006. http://www.americanchemistry.com/s_chemitc/sec.asp?CID=1636&DID=6196.
16. http://www.us-cert.gov/control_systems/icsjwg/.
17. http://www.us-cert.gov/.
18. http://www.us-cert.gov/control_systems/.
19. Multi-State Information Sharing and Analysis Center, http://www.msisac.org/about/.
20. US-CERT, Control Systems Cyber Security Awareness, *Informational Focus Paper*, July 2005, http://www.us-cert.gov/reading_room/Control_System_Security.pdf.



21. Chemical Sector Cyber Security Program Steering Team, *U.S. Chemical Sector Cyber Security Strategy*, American Chemistry Council, September 2006. http://www.americanchemistry.com/s_chemitc/sec.asp?CID=1636&DID=6196.

22. Welander, Pete, *10 Control System Security Threats, Control Engineering*, April 1, 2007 (Control Engineering-2007), http://www.controleng.com/article/269570-10_Control_System_Security_Threats.php.

23. GAO-04-354, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, March 2004, http://www.gao.gov/new.items/d04354.pdf.

24. GAO-07-1036, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, September 2007.

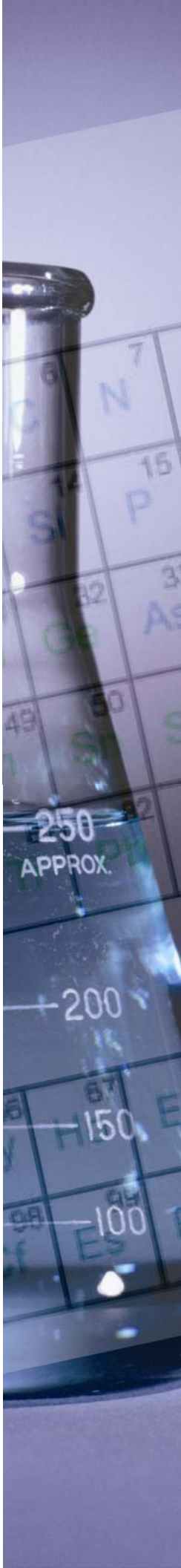
25. Internet Security Alliance, Cyber Security Social Contract Policy Recommendations for the Obama Administration, November 2008, http://www.isalliance.org/images/stories/The_Cyber_Security_Social_Contract_11182008.pdf.

26. Control Systems Cyber Security Self Assessment Tool (CS2SAT), http://csrp.inl.gov/Self-Assessment_Tool.html.

27. ISA Security Compliance Institute, http://www.isa.org/Content/NavigationMenu/Technical_Information/ASCI/ISCI/ISCI.htm.

ACRONYMS

ACC	American Chemistry Council
AGA	American Gas Association
ANSI	American National Standards Institute
API	American Petroleum Institute
BCIT	British Columbia Institute of Technology
CFATS	Chemical Facility Anti-Terrorism Standards
CFR	Code of Federal Regulations
ChemITC	Chemical Information Technology Center
CIH	Chen Ing-Hau (creator of the Chernobyl Virus)
CIKR	Critical Infrastructure and Key Resource
CIPAC	Critical Infrastructure Partnership Advisory Council
COTS	commercial-off-the-shelf
CS^2SAT	Control Systems Cyber Security Self Assessment Tool
CSCSP	Chemical Sector Cyber Security Program
CSCSWG	Cross-Sector Cyber Security Working Group
CSI	Computer Security Institute
CSSP	Control Systems Security Program
CSWG	Cyber Security Working Group
DCS	Distributed Control System
DHS	Department of Homeland Security
DOE	Department of Energy
E.O.	Executive Order
ES	Energy Sector
FBI	Federal Bureau of Investigation
FERC	Federal Energy Regulatory Commission (DOE)
FOUO	For Official Use Only
GAO	General Accounting Office
GCC	Government Coordinating Council
GTI	Gas Technology Institute
HSIN-CS	Homeland Security Information Sharing Network—Critical Sectors
HSPD	Homeland Security Presidential Directive
I3P	Institute for Information Infrastructure Protection
ICS	industrial control systems
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team



ICSJWG	Industrial Control Systems Joint Working Group
IP	Internet Protocol
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
IT	information technology
MS-ISAC	Multi-State Information Sharing and Analysis Center
NIAC	National Infrastructure Advisory Council
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NPRA	National Petrochemical & Refiners Association
PCII	Protected Critical Infrastructure Information
PCSRF	Process Control Security Requirements Forum
PDD	program description document
PL	Public Law
R&D	research and development
RBPS	Risk Based Performance Standards
ROI	return on investment
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SP	Special Publication
SPP-ICS	System Protection Profile for Industrial Control Systems
SSA	Sector-Specific Agency
Stds	Standards
UNIX	Computer Operating System
US-CERT	U.S. Computer Emergency Readiness Team
VoIP	Voice over Internet Protocol
WG	working group
WSCC	Water Sector Coordinating Council

Appendix 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 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.

The *Federal Information Security Management Act of 2002* requires that Federal agencies develop a comprehensive IT 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 SSP.

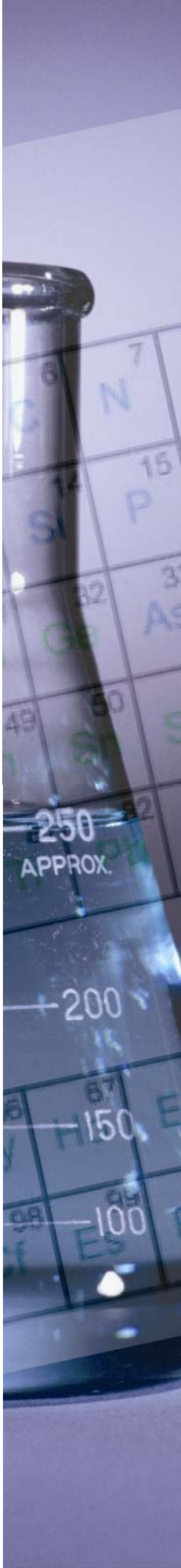
The *Cyber Security Research and Development Act of 2002* allocates funding to NIST and the NSF for the purpose of facilitating increased R&D for computer network security and supporting research fellowships and training. The act establishes a means of enhancing basic R&D related to improving the cybersecurity 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 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 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 (E.O) 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.

The NIPP was issued in 2006(updated in 2009). It establishes a partnership model for collaboration, consisting of a Sector Coordinating Council and a Government Coordinating Council for each sector consistent with the laws, directives, and strategies described above. The SSA for the Chemical Sector is DHS. The Chemical Sector collaborated with DHS to issue the 2007 Chemical SSP with a 2008 update. The Plan specifically addresses the cyber needs of ICS in the Chemical Sector.

CFATS (6 CFR § 27) issued on April 9, 2007, provides additional regulatory requirements on the Chemical Sector along with the call for performance based cybersecurity standards.

The NIPP provides a more extensive descriptive listing of laws, directives, and guidance for critical infrastructure protection, which includes those directed towards cybersecurity as well as other forms of risk.

Appendix B—Industrial Control Systems Security Issues and Challenges

The analysis behind this roadmap began by developing a list of issues obtained from a set of documents (see References) and sources that are widely available in the cybersecurity community:

- "CERT Information Focus Paper,"[18] 2005 (Cert-2005)
- Welander, Pete, "10 Control System Security Threats,: Control Engineering,"[22] April 1, 2007 (Control Engineering-2007)
- DHS CSSP program studies, evaluations, and experience including site assessments (CSSP)
- GAO-4-354, "Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems"[23]
- GAO-07-1036, "Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain"[24]
- GAO 08-113, "Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies"[6]
- Energy Sector Roadmap[1], 2006 (ES Roadmap).

This is not close to an exhaustive set of references, but the GAO reports, Energy Sector Roadmap, and CSSP represent the work and interviews of many of the active participants in the cyber ICS security community over the past six years. It probably represents a large percentage of the major concerns indentified by the Chemical Sector Roadmap Working Group.

Specific statements from these documents and sources that were phrased in the terms of issues, problems, or challenges were captured. This resulted in 228 issues. Issues that were clearly redundant were deleted; this resulted in the 140 issues shown in Table B-1. The remaining issues, which could be argued to be redundant, were left.

They were then categorized by "Type" of issue to develop a manageable set of issues. Some of the issues could clearly be placed in several "Types."

Table B-1 lists these 134 issues by type and source. The brief description of the issue is not intended to be an exhaustive statement of the issue. Individual and company names that may have been included in the source documents have been deleted from this list.

A list of challenges was developed from this list of issues. The distinction between issues and challenges is fuzzy at best. Roughly, issues are conditions that justify the need for enhanced cybersecurity and make it a larger problem than just installing the proper software or hardware. Challenges are more oriented towards the difficulties of implementing necessary security enhancements. We allowed for overlaps and some inconsistencies in these definitions. Issues must be addressed and challenges must be overcome in order to achieve the vision and goals of this roadmap.

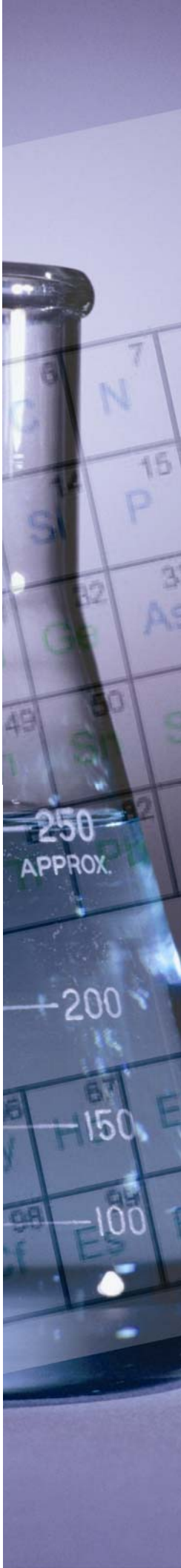


Table B-1. Cyber ICS security issues

No	Type	Source	Issue
1	Classified Information	CSSP	In addition to open technical and institutional information, any effective information sharing must be able to process and disseminate useful and actionable content from classified, proprietary, and FOUO (For Official Use Only) information.
2	Classified Information	CSSP	Classified information is restricted to a small circle.
3	Economic	CERT-2005	To reduce operational costs and improve performance, control system vendors and critical infrastructure owners and operators have been transitioning from proprietary systems to less expensive standardized technologies, operating systems, and protocols currently prevalent on the Internet.
4	Economic	ES RoadMap	Technology change is inhibited by lack of expertise, high costs, and corporate inertia.
5	Economic	ES RoadMap	The return on investment (ROI) for security cannot be demonstrated via any tangible measure; this applies to R&D, implementation, and time and effort.
6	Economic	ES RoadMap	Some decision-makers see no economic penalty associated with minimizing funding to deter cyber threats.
7	Economic	ES RoadMap	Assigning financial responsibility for security costs is problematic.
8	Economic	ES RoadMap	Designing and implementing new security features is a high-cost undertaking.
9	Economic	ES RoadMap	Limited resources are available within businesses to address security needs.
10	Economic	ES RoadMap	Even when risks, costs, and potential consequences are understood, it is difficult to make a strong business case for cybersecurity investment because attacks on ICS so far have not caused significant damage.
11	Economic	ES RoadMap	Cyber security is a difficult business case.
12	Economic	GAO-04-354	Securing ICS may not be perceived as economically justifiable.
13	Economic	GAO-07-1036	Difficulty in developing a compelling business case for improving ICS security.
14	Governmental	CSSP	Achieving uniform critical infrastructure cybersecurity enhancement without Federal regulations will require close cooperation with state and local government agencies.
15	Governmental	CSSP	Fear of a legislated solution.
16	Governmental	GAO 08-64T	Developing a comprehensive national plan for critical infrastructure protection, including cybersecurity.
17	Governmental	GAO-07-1036	The existing DHS cyber focuses primarily on DHS's initiatives. However, the strategy does not include ongoing work by DOE, FERC, NIST, and others. Further, it does not include the various agencies' responsibilities, goals, milestones, or performance measures.
18	Governmental	GAO-07-1036	(Lack of) an overarching strategy that delineates various public and private entities' roles and responsibilities and [failure to use] it to guide and coordinate ICS security activities, the Federal government and private sector risk investing in duplicative activities, and missing opportunities to learn from other organization's activities.
19	Governmental	GAO-07-1036	Lack of a rapid, efficient process for disseminating sensitive information to private industry owners and operators of critical infrastructures.
20	Governmental	GAO-07-1036	There is, as of 9/2007, no overall strategy to coordinate the various activities across Federal agencies and the private sector.
21	Information Sharing	CERT-2005	Significant information on ICS is now publicly available, including design and maintenance documents, technical standards for the component interconnections, and standards for communicating between devices.

Table B-1. (continued)

No	Type	Source	Issue
22	Information Sharing	CERT-2005	Widely accepted technologies, protocols, and operating systems, such as Ethernet, IP, Microsoft Windows, and web technologies, being used on or with ICS, have a large number of known cyber vulnerabilities, and new vulnerabilities are reported on a daily basis.
23	Information Sharing	CSSP	Coordination and information sharing must provide value added. It must be based on state-of-the-art knowledge in cyber risk analysis and cyber attack technology.
24	Information Sharing	CSSP	A staff capable of pushing the state of the art of hacking and prevention of hacking is necessary to effectively address the problem of control system cybersecurity. Only a Federally funded program has the luxury of devoting fully funded hackers to work towards maintaining the state of the art in hacking and retain these skills in a protected environment.
25	Information Sharing	CSSP	Information about infrastructures and ICS is publicly available.
26	Information Sharing	CSSP	Efforts to strengthen the cybersecurity of ICS are under way, but lack adequate coordination.
27	Information Sharing	CSSP	Limited control system security education and training.
28	Information Sharing	CSSP	Information Sharing and Analysis Centers (ISACs) are poorly coordinated.
29	Information Sharing	CSSP	Poor communication between stakeholders.
30	Information Sharing	CSSP-	Federal and private agency conflicts.
31	Information Sharing	CSSP	Infrastructure categories are not all inclusive.
32	Information Sharing	ES RoadMap	Coordination and information sharing between industry and government is inadequate, primarily due to uncertainties in how information will be used, disseminated, and protected.
33	Information Sharing	ES RoadMap	Outside the control system community, there is poor understanding of cybersecurity problems, their implications, and need for solutions.
34	Information Sharing	ES RoadMap	Information sharing is poor. When attacks occur, information about the attack, consequences, and lessons learned are often not shared beyond the company.
35	Information Sharing	ES RoadMap	Government information protection issues (e.g., Protected Critical Infrastructure Information and the Freedom of Information Act) and confidentiality concerns still linger.
36	Information Sharing	ES RoadMap	Effective security-oriented partnerships between government and industry have been difficult to establish.
37	Information Sharing	ES RoadMap	No secure mechanism exists for sharing information on threat vulnerabilities.
38	Information Sharing	ES RoadMap	Insufficient sharing of threat and incident information among government and industry entities.
39	Information Sharing	ES RoadMap	Poor coordination among government agencies creates confusion and inefficiencies.
40	Information Sharing	ES RoadMap	Limited knowledge, understanding, and appreciation of ICS security risks inhibit action.
41	Information Sharing	GAO 08-64T	Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities.

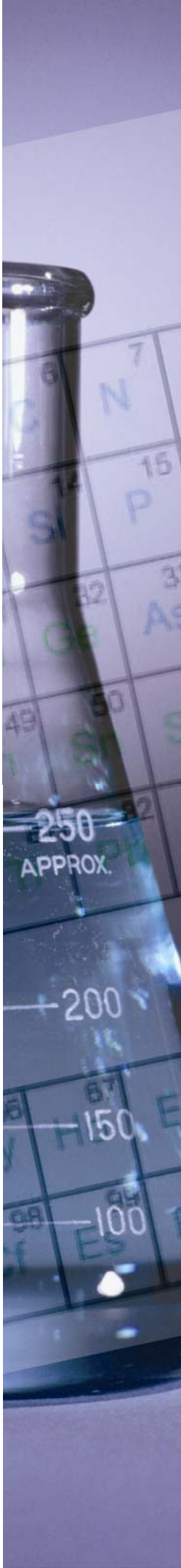


Table B-1. (continued)

No	Type	Source	Issue
42	Information Sharing	GAO-07-1036	Reluctance to share information on ICS incidents and the resulting lack of attention to this risk.
43	Information Sharing	GAO-07-1036	More needs to be done to address specific weaknesses in the ability to share information on ICS vulnerabilities.
44	Information Sharing	GAO-07-1036	There is a lack of processes needed to address specific weaknesses in sharing information on control system vulnerabilities. Until public and private sector security efforts are coordinated by an overarching strategy and specific information sharing shortfalls are addressed, there is an increased risk that multiple organizations will conduct duplicative work and miss opportunities to fulfill their critical missions.
45	Information Sharing	GAO-07-1036	Greater sharing of information on control system incidents could help build a business case.
46	Information Sharing	GAO-07-1036	There needs to be a focal point for the security of cyberspace— including analysis, warning, information sharing, vulnerability reduction, mitigation, and recovery efforts for public and private critical infrastructure information systems.
47	Institutional	CSSP	Cyber systems are international in character. The point of origin for an attack on a vulnerable system can be anywhere in the world, (for unprotected systems). Components and software are designed, manufactured, and maintained from many different countries. Many information systems are interconnected worldwide. Critical infrastructure is often owned, managed, and/or operated by international corporations.
48	Institutional	CSSP	Organizational priorities conflict.
49	Institutional	GAO 08-64T	Provide and coordinate incident response and recovery planning efforts.
50	Institutional	GAO 08-64T	Promote awareness and outreach.
51	Institutional	GAO 08-64T	Develop partnerships and coordinate with other Federal agencies, State and local governments, and the private sector.
52	Institutional	GAO-04-354	Organizational priorities conflict.
53	Institutional	GAO-04-354	Efforts to strengthen the cybersecurity of ICS are under way, but lack adequate coordination.
54	Institutional	GAO-04-354	Publicly available information about infrastructures and ICS increases risk because target information is available to threat actors.
55	Institutional	GAO-07-1036	Division of technical responsibilities within an organization.
56	Institutional	GAO-07-1036	Critical infrastructure owners face organizational challenges in securing ICS.
57	International	CERT-2005	ICS commonly used in the United States are also available to adversarial countries, providing adversaries an insider view of system components and software.
58	International	CERT-2005	Adversaries could dedicate time and resources to discovering vulnerabilities and developing exploits and then attempt to remotely gain access to critical U.S. ICS through an increasing number of potential access points.
59	International	GAO 08-64T	Strengthen international cyber space security.
60	Legacy Systems	CSSP	Insecure legacy systems.
61	Legacy Systems	ES RoadMap	New regulations may impose requirements beyond the functional capability of legacy systems. Highly educated staff with broad skill sets are needed to manage future operations.
62	Legacy Systems	ES RoadMap	Security upgrades are hard to retrofit to legacy systems, may be costly, and may degrade system performance.
63	Legacy Systems	ES RoadMap	Security upgrades for legacy systems may degrade performance due to the inherent limitations of existing equipment and architectures.

Table B-1. (continued)

No	Type	Source	Issue
64	Research and Development	CSSP	Many errors, cyber events, and incidents are human-factor related. A study by Jason Stamp/SNL/2003 pointed out that cyber control system vulnerabilities were traceable to human factors.
65	Research and Development	CSSP	R&D efforts and initiatives to develop control system security measures and improve the secure of control system components are lacking
66	Research and Development	GAO 08-64T	Efforts to promote and support research and development efforts to strengthen cyber space security are lacking.
67	Risk	CSSP	The control system cyber threat landscape consists of many potential attackers, with multiple industries, targets, vendors, significant countries, and Federal agencies all at risk of attack or compromise.
68	Risk	CSSP	Additional efforts are needed to fund and develop of risk scenarios for control systems, an integral component in safety and reliability studies supporting the design and operation of nuclear, chemical, and hazardous material handling facilities.
69	Risk	CSSP	During the course of speaking with CIKR owner/operators in 2005 and 2006, a major concern was repeatedly voiced: "how do we know that components (microelectric hardware in particular) manufactured in foreign countries, some known to have or support terrorist groups, do not contain security bugs designed and built into them?"
70	Risk	CSSP	ICS can be vulnerable to cyber attacks, and cyber attacks have been reported.
71	Risk	CSSP	Limited documented and reported historical evidence of cyber attacks on ICS.
72	Risk	ES RoadMap	Security stakeholder roles and responsibilities are not clearly understood.
73	Risk	ES RoadMap	Identifying strategic risks to ICS is complicated by the proprietary nature of vulnerability assessments, the lack of adequate and reliable threat information, and difficulties in determining the return on security investments—particularly in rate-regulated energy industries.
74	Risk	ES RoadMap	Security measures affect the ability to respond quickly in emergencies.
75	Risk	ES RoadMap	No clear vision of the threat has been articulated.
76	Risk	ES RoadMap	Most organizations lack existing groups, teams, or committees that bring together the right mix of people or fields of expertise to find solutions.
77	Risk	ES RoadMap	Security awareness has not been a priority in system development and use.
78	Risk	GAO 08-64T	Enhance Federal, State, and local government cybersecurity.
79	Risk	GAO 08-64T	Develop and enhance national cyber analysis and warning capabilities.
80	Risk	GAO 08-64T	Support efforts to reduce cyber threats and vulnerabilities.
81	Risk	GAO 08-64T	Identify and assess cyber threats and vulnerabilities.
82	Risk	GAO-04-354	Cyber attacks on ICS have been reported.
83	Risk	GAO-04-354	ICS can be vulnerable to cyber attacks.
84	Standards (Stds)/Metrics/ Training	CSSP	New guidance for performance based cybersecurity standards are required by this new regulation.
85	Stds/Metrics/ Training	CSSP	Communication between many different government agencies and thousands of private industries and corporations requires a common set of metrics for use in specifying risk, measuring security levels, and determining cybersecurity performance measures. Such a set of metrics does not exist. According to the NIPP, Section 2.2.1, DHS is responsible for "…recommending risk management and performance criteria and metrics within and across sectors."
86	Stds/Metrics/ Training	CSSP	Lack of mature and consistant cybe security standards for control systems across the various critical infrastructure sectors.

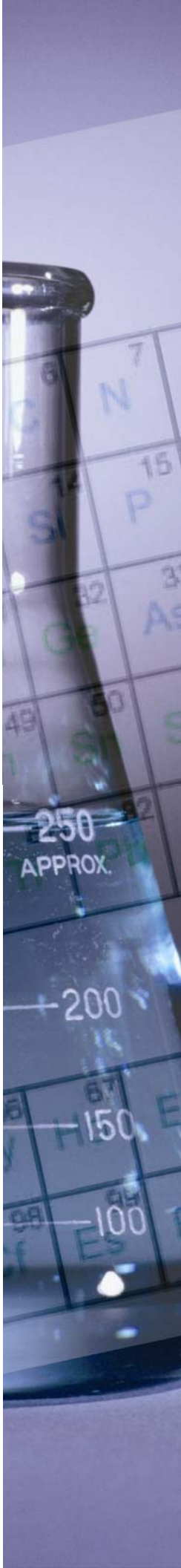


Table B-1. (continued)

No	Type	Source	Issue
87	Stds/Metrics/ Training	ES RoadMap	Many companies lack consistent metrics or reliable tools for measuring their risks and vulnerabilities.
88	Stds/Metrics/ Training	ES RoadMap	Standardized test plans and upgrades for new technology are not widely available.
89	Stds/Metrics/ Training	ES RoadMap	Vendors do not have specific requirements or standards to build to.
90	Stds/Metrics/ Training	ES RoadMap	Tested and validated security tools are lacking.
91	Stds/Metrics/ Training	ES RoadMap	Many companies today have limited ability to measure and assess their cybersecurity posture.
92	Stds/Metrics/ Training	ES RoadMap	Clear security design requirements are lacking.
93	Stds/Metrics/ Training	GAO 08-64T	Foster training and certification.
94	Threat	ES RoadMap	Threats, when known, are often difficult to demonstrate and quantify in terms that are meaningful for decision makers.
95	Threat	ES RoadMap	Cyber intrusion tools are becoming increasingly sophisticated.
96	Threat	GAO-07-1036	Hacktivism refers to politically motivated attacks on publicly accessible webpages or e-mail servers. These groups and individuals overload e-mail servers and hack into websites to send a political message.
97	Threat	GAO-07-1036	Virus writers are posing an increasingly serious threat. 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, and Code Red.
98	Threat	GAO-07-1036	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. However, traditional terrorist adversaries of the United States are less developed in their computer network capabilities than other adversaries. Terrorists likely pose a limited cyber threat. The Central Intelligence Agency believes terrorists will stay focused on traditional attack methods, but it anticipates cyber threats will grow with a more technically competent generation.
99	Threat	GAO-07-1036	The disgruntled insider, working from within an organization, is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes contractor personnel.
100	Threat	GAO-07-1036	There is an increased use of cyber intrusions by criminal groups that attack systems for monetary gain.
101	Threat	GAO-07-1036	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. Also, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the CIA Director, can affect the daily lives of all Americans.
102	Threat	GAO-07-1036	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, attack tools have become more sophisticated and easier to use.

Table B-1. (continued)

No	Type	Source	Issue
103	Vulnerability	CERT-2005	Vast information technology expansion and the drive towards having information readily available from any location is generating new vulnerabilities within the sector. Many previously stand-alone ICS are being transitioned to the always connected world, where real-ICS information can be readily and easily accessed remotely by vendors, engineers, maintenance personnel, business managers, and others via corporate networks, the Internet, telephone lines, and various wireless devices. This leads to new vulnerabilities.
104	Vulnerability	CERT-2005	ICS are typically not up to date with the latest security patches, fixes, and industry accepted practices due to concerns with taking real-time systems offline and concerns over making system modifications that might affect the time sensitive operations of the control system, or potentially affect existing agreements with control system vendors or others.
105	Vulnerability	CERT-2005	Exploitation tools, worms, and how-to papers are often readily available shortly after the announcement of a new vulnerability.
106	Vulnerability	Control Engineering-2007	Some of the most common ways to compromise a system involve problems with poor coding practices, such as using static buffers or libraries that clearly have vulnerabilities. Ocassionally developers rely on some sort of 'tool' to analyze source code once written; this means vulnerability detection is limited to the capabilities and patch level of the tool. Coding standards and writing secure code are available disciplines today, and should be followed. End-users, system integrators, and consultants should all insist upon rigorous application testing, viewing coding standards for vendors, etc. Steinberg warns that some flaws will always remain: "There is no way to remove all of the code flaws from these systems, nor create all known good and bad test cases. The best way to mitigate the potential for problems is to minimize the application set complexity, perform a rigorous review of operating system and application code, and avoid interpreted solutions when possible. Depending upon cost and time, it also makes sense to generate two application sets using two different development teams to minimize the potential for injecting the same logic flaws."
107	Vulnerability	Control Engineering-2007	Problems with wireless technologies fall into four basic areas: unauthorized use, on-air interception, frequency interference, and unauthorized extension.
108	Vulnerability	Control Engineering-2007	System updates, user metrics, and the like are not part of the control system implementation. This vulnerability goes back to the people who are running the ICS whose core competencies may not be in the IT area; the vulnerabilities that are discovered in these systems are often IT-related. There needs to be a capability in place that indicates 'what's the latest thing added to the system or what's changed since the last time the system was running properly.
109	Vulnerability	Control Engineering-2007	Terminal services, wireless networks, radio telemetry equipment, modems, and unsecured computers abound. Where electronic security is not feasible, there needs to be good physical security. This also extends into the capability to detect rogue or additional devices. Most networks are not managed or configured to stop unauthorized devices, so additional ICS, PCs, or even attackers' workstations can often be joined to the network and never detected.

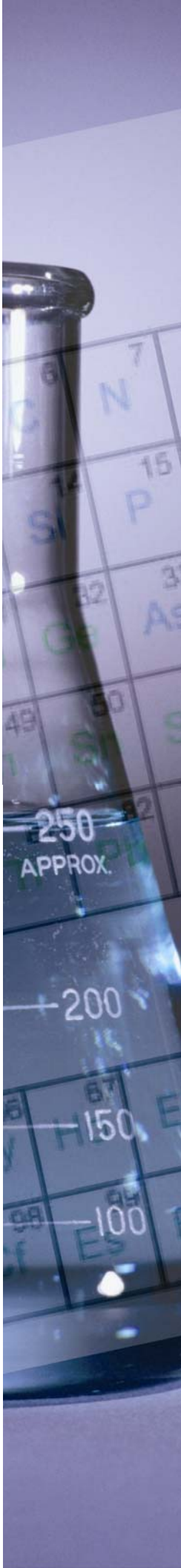
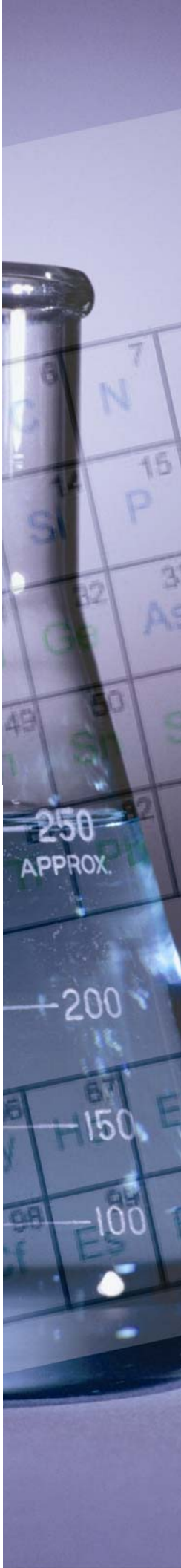


Table B-1. (continued)

No	Type	Source	Issue
110	Vulnerability	Control Engineering-2007	Many IT folks have bought the 'converged network' line and think it's OK. Cameras, VoIP, business systems processing payroll, and a whole host of other issues have caused denial of service conditions on control networks. IT professionals typically look at application performance, and near real time for control is a foreign concept. Taking 300-500 ms extra to receive e-mail or a Webpage is largely unnoticeable; 300-500 milliseconds for control messages or safety messages could be disastrous. Often, what is an acceptable level of saturation or utilization from an IT perspective can spell disaster for controls.
111	Vulnerability	Control Engineering-2007	Defense requires more than just a strong perimeter. To secure a control system successfully requires taking a systematic and comprehensive approach. One of the most common (and dangerous) misunderstandings is that by simply installing a control system firewall, the system is protected. Instead, a layered approach called defense-in-depth is recommended. Defense-in-depth advocates the creation of a nested security architecture whereby the plant is divided into multiple secure and closed cells (zones). Each cell must have clearly defined and monitored access points to control access and communication in and out. ICS must have hierarchical levels of protection. The more critical the access, like controls and HMI, the deeper it needs to be defended. ICS at a minimum should be firewalled off from the business network, and they should never be allowed to access the Internet.
112	Vulnerability	Control Engineering-2007	The systems also needs adequate forensic and audit methods. Risk mitigation tools include perimeter protection (firewall, anti-virus, intrusion protection, content filtering, etc.), network intrusion detection (scanning the network for intrusions, rogue devices, changes in traffic levels, etc.), host intrusion detection (detecting file/process/socket changes, monitoring message queues, login failures, removable media insertion, abnormal exits, etc.), and performance monitoring.
113	Vulnerability	Control Engineering-2007	Security begins with a culture and mindset of all those involved. There is a tendency to think of security in terms of a technical solution: firewalls and passwords. While those elements may cover 20% of the overall solution, common sense approaches to security implemented by plant personnel should make up the remaining 80%. The facility needs a security policy, including human access control and controls on outside portable media (hardware and software) of all kinds. Without an effective security policy that addresses procedures, mitigation strategies, and periodic training, all other security programs are less successful. To be successful, security must be viewed as an ongoing process, not a one-time investment into firewalls, intrusion prevention or detection, encryption technologies, etc.
114	Vulnerability	Control Engineering-2007	The control system needs to safely and effectively control the process. Only necessary applications that are directly involved with the control of the process should be installed. All unnecessary applications should be removed and addition of new programs rigidly controlled.

Table B-1. (continued)

No	Type	Source	Issue
115	Vulnerability	Control Engineering-2007	Not all controllers out there today authenticate who's making the change and authorize that the change is allowed for that user through the controller. This security step on most ICS is performed at a layer in the control system above the controllers. This leaves the controllers vulnerable, and that's why defense-in-depth is absolutely required. Controllers should be deep down in the security infrastructure, with multiple layers of defense above them, otherwise the controllers are basically wide open on the Web. Steinberg stresses people management: "When it comes to authenticating command and control, the only choice that providers have is to augment the human aspect, specifically with respect to problem analysis, chain of command, and communication flow. Proper policy, practice, and procedure will buy time for older command infrastructures to be re-thought and replaced."
116	Vulnerability	CSSP	ICS are connected to business and business networks ,which require protective measures to isolate the ICS.
117	Vulnerability	CSSP	ICS are adopting standardized software operating platforms which are suspectable to common vulnerabilites and require regular patching and updates
118	Vulnerability	ES RoadMap	Open and flexible control leads to increased risks.
119	Vulnerability	ES RoadMap	Poorly designed connections between ICS and business networks introduce further risks.
120	Vulnerability	ES RoadMap	ICS are becoming increasingly interconnected and often operate on open software platforms with known vulnerabilities and risks.
121	Vulnerability	ES RoadMap	Sophistication of hackers' tools and resources is increasing.
122	Vulnerability	ES RoadMap	Complexity increases exponentially with an increase in number of nodes.
123	Vulnerability	ES RoadMap	There are known technical vulnerabilities in non vendor supported) hardware and software.
124	Vulnerability	ES RoadMap	Poorly designed connection of ICS and business networks can dramatically increase vulnerabilities of ICS.
125	Vulnerability	ES RoadMap	New architectures with built-in, end-to-end security will take years to develop and even longer to deploy throughout the sector.
126	Vulnerability	GAO-04-354	Insecure connections exacerbate vulnerabilities.
127	Vulnerability	GAO-04-354	ICS are connected to other networks.
128	Vulnerability	GAO-04-354	ICS are adopting standardized technologies with known vulnerabilities.
129	Vulnerability	GAO-07-1036	Increased connectivity of ICS to other computer networks and the Internet.
130	Vulnerability	GAO-07-1036	Potential to interfere with critical infrastructure operations from remote locations.
131	Vulnerability	GAO-07-1036	ICS configured with remote access through either a dial-up modem or over the Internet to allow remote maintenance or around-the-clock monitoring.
132	Vulnerability	GAO-07-1036	Insecure connections.
133	Vulnerability	GAO-07-1036	Increased standardization of technologies.
134	Vulnerability	GAO-07-1036	Widespread availability of technical information about ICS enables attackers to plan and conduct their attack often with detailed information, which may include design drawings, photographs, and policy, procedure, and operating manuals.



Each challenge was matched to a single goal; this was subjective, but it provides a grouping that gives the general idea of challenges blocking the achievement of each goal. The result is the list of 57 challenges shown in Table B-2.

Table B-2. Cyber ICS Security Challenges

Goal	Source	No	Challenge
Measure and assess security posture	Chemical Sector Cyber Strategy	1	A cyber attack on a vulnerable ICS could result in business interruption, loss of capital, and impacts to plant employees, public safety, the environment, and national security.
	CS Roadmap WG	2	Inventory of critical assets, their associated ICS, and the risk of cyber attack are often not adequately known or understood.
		3	Practical and cost-efficient assessment tools are needed but not widely available.
		4	Knowledge and understanding of risk (including threat, vulnerability, defense, and consequence) analysis capabilities across the sector is limited.
		5	Metrics to measure cybersecurity posture and/or improvements over time and across the sector are available, but not widely used within the sector.
		6	Security vulnerability assessments are needed to determine the consequences of specific cybersecurity compromises of ICS.
	ES RoadMap	7	Security metrics are required to perform detailed threat analyses.
		8	Existing standards lack meaningful and measurable specifications relating to ICS cybersecurity.
		9	Cyber security threats are difficult if not impossible to quantify, but quantified values are required for quantified risk estimation.
		10	Cyber risk factors are neither widely understood nor accepted by technologists and managers.
		11	Current standards for assessment of cyber vulnerabilities are inadequate.
		12	Consistent metrics are necessary but not available to measure and assess security status.
Develop and integrate protective measures	CERT-2005	13	Widespread and continuous connectivity of IT and ICS, and generally with remote access by multiple parties or devices, provides opportunity and routes for cyber attack.
	Control Engineering-2007	14	Many ICS operate using unauthenticated command and control data.
		15	Many ICS have remote access points without appropriate or adequate access control.
	CS Roadmap WG	16	Many ICS have been designed, built, and operated within open communication environments.
		17	The unavailability of patch management that conforms to a 24/7 production environment with extended vulnerability windows and without regularly scheduled maintenance opportunities leads to windows of opportunity for cyber attack on systems with known but unfixed vulnerabilities.
		18	Older operating platform (legacy and hybrid) systems may have limited or no vendor/service support, thus limiting their ability to secure the systems.
	CSSP	19	Existing ICS with numerous access points, default vendor accounts/passwords/shared passwords, and poor firewall implementation provide increased cyber attack opportunities.
		20	Basic security features are often not enabled.
	ES RoadMap	21	The complexity of ICS increases exponentially with an increase in the number of nodes, thereby increasing attack opportunities.
		22	Security upgrades are hard to retrofit to legacy ICS, may be costly, and may degrade system performance, thus lessening incentive to upgrade those systems.
		23	Risks can arise from using nonvendor hardware and software.

Table B-2. (continued)

Goal	Source	No	Challenge
Detect Intrusion and implement response strategies	CSSP	24	Periodic and appropriate reviews of security logs and change management documentation often receives limited if any attention.
	ES RoadMap	25	Cyber security measures may negatively impact rapid response to emergencies.
		26	The continual increase in the sophistication of hackers tools and resources increases attack risk.
Sustain security improvements	Chemical Sector Cyber Strategy	27	Necessary and constructive relationships with governmental authorities for the availability, reliability, and accessibility of threat information for the sector are often lacking.
		28	Cyber security has too often been handled separately for more traditional company security and safety programs.
		29	Federal legislation to enhance national cybersecurity guidelines for chemical facilities that proceeds with limited input from owner/operators will create implementation problems.
	Control Engineering-2007	30	Inadequate policies, procedures, and culture relating to ICS cybersecurity negatively impacts security and increases risk.
	CS Roadmap WG	31	Chemical facilities often have toxic, flammable, and explosive chemicals that provide attractive targets for terrorists to release, steal, or sabotage.
		32	Without active input from owner/operators, cost efficient compliance with 6 CFR 27 that is consistent across the sector and adequate and appropriate to the risk-based tier level for each facility will be difficult to achieve.
		33	Differing business models and risk profiles within the same operational boundaries (not all parts of a given plant have the same potential for severe consequences) increases the difficulty and incentives to implement cybersecurity measures.
		34	Discovery of vulnerabilities, improved awareness, implementation of protective measures, and application of continuous improvement relative to cybersecurity is necessary to stay ahead of potential cyber attackers.
		35	Funding and implementation of enhanced security measures is difficult without executive recognition of ICS security threats and liabilities.
		36	Implementation of cyber-security across the entire sector is difficult due to varying needs of asset owners, and there is a large number of different asset owners.
		37	Funding of activities (R&D, for example) important to ICS security depends on input from industry to properly align government and industry goals.
		38	Consistent standards, requirements, and guidance from sector-specific agencies is limited or lacking.
		39	The Chemical Sector has a significant diversity of processes and products (>70,000 products), which increases both the risk to and the difficulty of enhancing ICS cybersecurity.
		40	Dissemination of ICS security information to the large number of asset owners in the Chemical Sector with diverse interests is complicated.
		41	ICS cybersecurity across the many types of production facilities within the sector is currently not always based on industry accepted practices.
		42	Traditionally there has been a collaboration barrier between IT and ICS departments that can lead to inconsistent and redundant security measures.

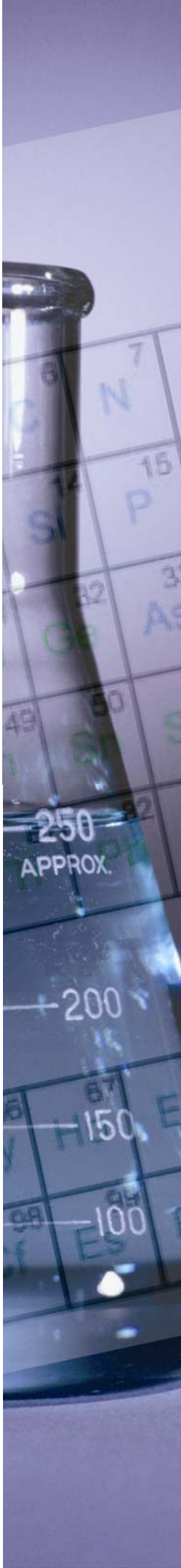


Table B-2. (continued)

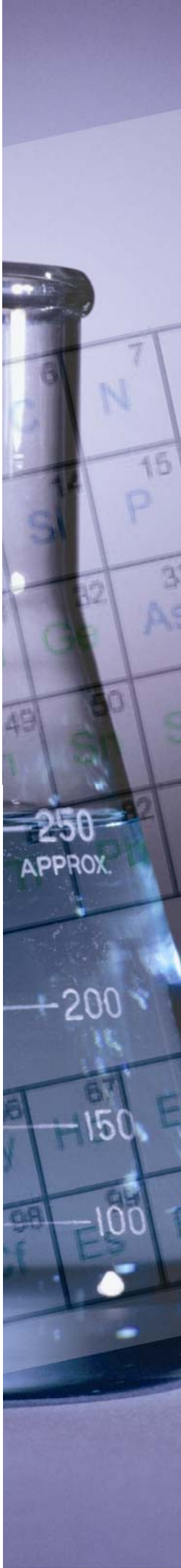
Goal	Source	No	Challenge
Sustain security improvements (continued)	ES RoadMap	43	Poor coordination among government agencies creates confusion and inefficiencies.
		44	New regulations may impose requirements beyond the functional capability of legacy systems.
		45	Limited knowledge, understanding, and appreciation of security risks inhibits constructive, necessary, and sufficient cybersecurity enhancement and implementation.
		46	A cybersecurity business case based on enhanced risk analyses, which could quantify and prioritize necessary and sufficient security measures and justify costs, is required but not available.
		47	Effective security-oriented partnerships between government and industry have been difficult to establish.
		48	Asset owners fear the loss of intellectual property rights by widely and openly sharing incident and assessment information related to enhanced ICS security measures.
		49	Inadequate and insufficient sharing of cyber threat and incident information between government and industry negatively impacts the ability to properly assess risk and select appropriate cybersecurity measures.
Secure-by-design	CERT-2005	50	The increasing use of standardized ICS increases attack opportunity.
	CS Roadmap WG	51	Enhanced cybersecurity upgrades on ICS with long design lives that were not initially designed for current cybersecurity requirements may be difficult and not obviously cost efficient.
		52	Security that is not necessarily integrated into a vendor's ICS products increases inherent vulnerabilities, requires retrofits and upgrades, and still results in a less secure system.
	ES RoadMap	53	Poorly designed interconnections between ICS and business networks can dramatically increase vulnerabilities and attack opportunities.
		54	Standardized security test plans and upgrades for all new-technology systems and components are not widely available, if at all.
		55	Tools and techniques sufficient to quantify or measure risk do not exist.
		56	Vendors do not have adequate requirements or standards to design and build cybersecurity into ICS.
		57	Tested and validated cybersecurity tools for ICS are lacking.

The literature search resulted in more than 200 separate, but not necessarily unique "challenges," which were then grouped into the challenge categories shown in Table B-3.

Table B-3. Categorical Grouping and Brief Description of Challenges

	No.	Challenge Category	Description of Challenge Category*
The Problem	1	System Vulnerability	Accessibility and ICS vulnerabilities. Technical ability of adversaries to gain access and ultimately control of a cyber system, including physical access, wireless communications, open systems, and public availability of system information.
	2	International	Off-shoring and outsourcing; international partners, or facilities; the international nature of cyber threat; foreign manufacture of cyber ICS and system components.
	3	Risk analysis (lack of)	Risk assessment and analysis; adequate understanding of threats, vulnerabilities, system assets, technical security metrics, and scenarios leading from attack to final incident consequences.
	4	Business case	Economic justification for security enhancements, incentives, and insurance.
The Solution	5	Risk analysis and assessment	System assessment, risk assessment and analysis. Defining and understanding the details of cyber threat, attack, defense, protection, and recovery.
	6	Design	System complexity; legacy and installed systems; availability of tools; availability of secure systems for procurement, the degree to which security is designed into those systems, the quality assurance that the systems function as intended; research and development into more secure system design and future generations of secure systems; research into improved usability of security features.
	7	Implementation	Putting available security systems in service, monitoring and auditing security systems, funding security efforts, human factors, organizational and management metrics relating to security implementation, and patch management.
	8	Standards	Identification and availability of Industry accepted practices, development of security standards, compliance to regulations (CFATS, for example) and implementation guidance.
	9	Training	Training in security practices, cybersecurity education, awareness of security issues, technological knowledge, and other items that might be resolved by enhanced training and education.
Coordination	10	Information sharing	Inter- and intra-sector sharing, incident reporting, and sharing of information between government owner-operators, and vendors.
	11	Working together	Working with government agencies, other companies, standards and regulatory bodies

* Many challenges are stated with qualifiers such as, "lack of, difficulty, need to, etc." The negative qualifiers have been dropped for simplicity. This makes many of the challenges appear to be solutions.



Appendix C—Chemical Sector Priorities

This appendix presents a tabular listing of priorities developed from the issues and challenges followed by a table of the milestones, based on priorities. The milestone table provides a comparison between the Energy Sector Roadmap milestones and the Chemical Sector Roadmap milestones, along with brief commentary for each milestone that addresses the milestone objective, existing capabilities related to that milestone, and gaps to be addressed in achieving that milestone.

PRIORITIES

The list of priorities was constructed by beginning with those from the *Energy Sector Roadmap*. Then priorities specific to the interests of the Chemical Sector were added. The challenges were reviewed to verify that all challenges were addressed by one or more priority. In the following tables, the priorities taken from the Energy Sector Roadmap are highlighted in blue. Limited comments are included below each table to address a new priority.

GOAL 1

The priorities for Goal 1, Measure and Assess Security Posture, are listed in Table C-1.

Table C-1. Priorities for Goal 1

Number	Measure and Assess Security Posture Priorities
1	Create a risk matrix that balances threat, vulnerability, and consequence
2	Analyze risk and determine what action is appropriate
3	Continue to fund efforts to enhance tool sets for owners and operators to conduct self assessments and encourage usage of those tools.
4	Set up and evaluate cyber attack and response simulators
5	Develop consensus on clear and concise metrics for measuring security posture
6	Develop risk assessment tools that include vulnerability assessment methodologies, frameworks for prioritizing control measures, and cost justification tools
7	Improve security requirements defined across system life cycles for fundamental, intermediate, and advanced security posture
8	Develop automated security state and response support systems
9	Create an environment for securely sharing collected U.S. Government information on threats and real-world attacks with utilities and vendors
10	Encourage participation with HSIN-CS

DHS has implemented the Homeland Security Information Sharing Network—Critical Sectors (HSIN-CS). This is a robust suite of information sharing and reporting tools designed to foster communication and cooperation between DHS and critical infrastructure sectors. HSIN-CS enables registered users to receive, submit and discuss timely and practical information and communicate information pertaining to threats, vulnerabilities, security, response, and recovery activities. HSIN-CS is intended to be the primary information sharing mechanism between DHS and critical infrastructure sectors, but is not, however, the cyber incident reporting site (see http://www.dhs.gov/).

GOAL 2

The priorities for Goal 2, Develop and Integrate Protective Measures, are listed in Table C-2.

Table C-2. Priorities for Goal 2

Number	Develop and Integrate Protective Measures Priorities
1	Identify accepted industry practices for physical and cybersecurity of control centers
2	Develop cost-effective gateway security that includes firewalls, intrusion detection, and anti-virus protection with minimum host impact
3	Develop a security test harness with testing architecture and guidelines
4	Maintain government test/assessment centers to work with vendors and asset owners to test equipment, architectures, and processes for both cyber and physical security
5	Develop patching technologies that do not impact 24/7 operations of operating systems
6	Improve performance of legacy communications to enable the application of security solutions
7	Identify industry accepted practices for connecting ICS and business networks
8	Put nonintrusive, cost effective, and robust ICS encryption solutions into production
9	Develop hardened operating systems for the ICS environment

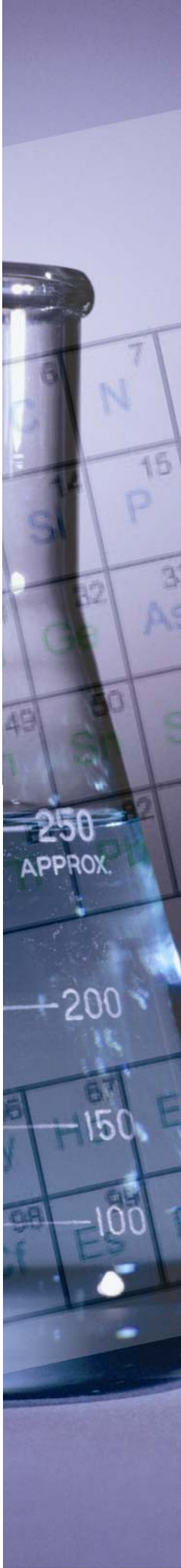
GOAL 3

The priorities for Goal 3, Detect Intrusion and Implement Response Strategies, are listed in Table C-3.

Table C-3. Priorities for Goal 3

Number	Priorities
1	Develop and deploy sensors and sensor systems with mechanisms to detect and report anomalous activity
2	Develop automated security state and response support systems
3	Identify industry-approved incident reporting guidelines and industry accepted practices
4	Expedite security clearances for industry to facilitate information sharing and incident reporting
5	Develop and provide training on incident response procedures and tools
6	Adapt intrusion prevention systems for more robust application to networks and hosts
7	Develop tools for security event management
8	Enable automated collection of security information, including incident reports and visualization tools for correlation
9	Develop intrusion detection system/intrusion protection system products for ICS and audit trails with automated reporting
10	Designate a staff member at each chemical industry facility with responsibility to utilize, maintain, or support cyber ICS as the ICS-CERT/US-CERT contact point

Priority 10 is important because the US-CERT is a central location to obtain information specific to cyber vulnerabilities and to report cyber attack incidents. The primary site, http://www.us-cert.gov/, addresses cyber vulnerabilities. The control system specific site address, http://www.us-cert.gov/control_systems/ is dedicated to control system security issues. The Chemical Sector will encourage all of its members to maintain periodic links to the US-CERT Control Systems website and



work with ICS-CERT/US-CERT to report cyber vulnerabilities. A staff member with responsibility to utilize, maintain, or support cybersecurity of ICS at each chemical industry facility should be designated as the ICS-CERT/US-CERT contact point.

GOAL 4

The priorities for Goal 4, Sustain Security Improvements, are shown in Table C-4.

Table C-4. Priorities for Goal 4

Number	Priorities
1	Develop standards and/or regulations for secure data exchange and communications
2	Analyze incentives and benefits of implementing security to help fortify the business case
3	Create appropriate incentives to invest in ICS security
4	Create a cost-shared ICS security consortium that is protected from anti-trust issues
5	Develop and implement security training for all employees and contractors
6	Develop curricula and university programs to improve education and ICS, security and risks, and associated economics
7	Facilitate information sharing by guaranteeing protection of industry critical infrastructure protection information through legislation or other means
8	Encourage participation in supported industry activities
9	Direct official interaction with the DHS through Chemical SCC security activities, particularly ISA99 Industrial Automation and Control Systems Security
10	Work with the government to develop cyber risk methodologies consistent with the needs and interests of the Chemical Sector
11	Host two sector-specific cybersecurity networking meetings each year
12	Periodically review and assess existing guidance documents to evaluate their relevancy under current conditions, and incorporate emerging needs and potential enhancements

Priorities 8–10 recommend direct interface and cooperation with organizations specifically structured or committed to enhancing security of ICS, specifically ISA, PCSRF, CSCSWG, ICSJWG, the CSSP, and the government. Priority 11 recommends periodic meetings to support commitment to this roadmap. Priority 12 is a standard action to support currency within any field.

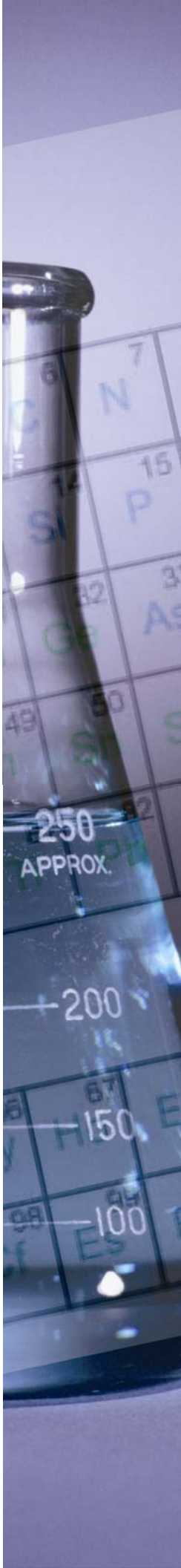
GOAL 5

The priorities for Goal 5, Secure-by-Design, are shown in Table C-5. This goal did not appear in the *Energy Sector Roadmap*. Priority 1 in the *Energy Sector Roadmap* was placed under Goal 2.

Goal 5 has three key thrusts: have vendors design and build security into systems, establish a culture in which the owner/operators request that designed and procured systems and components are secure, and develop independent certification centers that can verify the inherent security of a system or component.

Table C-5. Priorities for Goal 5

Number	Priorities
1	Develop true plug-and-play components that are secure
2	Strive for ICS products that are secure-by-design
3	Specify systems that are secure-by-design when procuring or upgrading new systems
4	Work with vendors where possible to assist in achieving the secure-by-design goal
5	Increase automation in the technical implementation of cybersecurity policies, procedures, and practices
6	Establish a certification center with the initial capability to demonstrate that cyber ICS and components meet established security standards and evolving to a capability to demonstrate systems and components secure-by-design



Appendix D—Chemical Sector Milestones

Chemical Sector Roadmap milestones grouped by Goal are presented in Table D-1. The dates in the "Date" column are anticipated completion years. The right-hand column discusses the milestone objective, existing capabilities toward achieving the milestones, and known gaps that need must be addressed before the milestone can be achieved. This discussion of objectives, existing capabilities, and gaps is not intended to be comprehensive, but captures the Chemical Sector Roadmap Working Group discussions during the milestone development process.

Table D-1. Chemical Sector Roadmap Milestones

Goal	No.	Milestone	Date	Commentary
Measure and assess security posture	1.1	Establish an industry-driven awareness effort to communicate information relating to the cybersecurity threats, vulnerabilities, and risks and the availability of accepted practices, tools, and training materials to the Chemical Sector.	2009	Objective: Make asset owners and operators aware of cyber risk and security enhancements; provide owner/operators with necessary information to improve their security posture. Existing Capabilities: The CSSP Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT), US-CERT Secure Portal, Industrial Control Systems Joint Working Group (ICSJWG), Sector Coordinating Council (SCC), Chemical Information Technology Center (ChemITC). Material is available from the Control Systems Security Program (CSSP) and many commercial companies at present. NIST Special Publication (SP) 800-82 (Draft September 2008) provides a detailed description of ICS security and a guide to NIST standards applicable to Information Technology (IT) security. International Society of Automation (ISA); ISA-TR 99.00.01 and ISA-TR 99.00.02 and ISA Standards 99-Part 1 and 2 are available. Gaps: Asset owner participation is lacking. NIST ICS Standard 800-82 is still a draft. ISA-99 Part 3 and Part 4 have not been written.
	1.2	Metrics for benchmarking security posture are available and agreed upon.	2010	Objective: Provide uniform means to measure the degree to which cybersecurity is implemented on an ICS. Existing Capabilities: The CSSP Control System Cyber Security Self-Assessment Tool (CS^2SAT) [http://csrp.inl.gov/Self-Assessment_Tool.html] is available and can be used to baseline the ICS security posture to currently available security standards and accepted practices. NIST published the Performance Measurement Guide (SP 800-55 Rev. 1) in July 2008, to assist in the development, selection, and implementation of security metrics based on the SP 800-53 security measures. It describes a method for performing a measurement, but leaves the metrics choice to the user to select from NIST SP 800-53, 53A and Draft 82. SP 800-82, neither of which lists performance metrics. Gaps: Currently there is no generally agreed upon metrics other than those from NIST. The ISA-99 Part 2 Standard, which contains information about what constitutes an "effective" ICS cybersecurity program. Chemical sector agreement on which metrics to use will need to be addressed.
	1.3	Asset owners and operators are performing self-assessments of their ICS using consistent criteria.	2012	Objective: Determine what is required for adequate ICS security for a system. Existing Capabilities: The CSSP CS^2SAT (http://csrp.inl.gov/Self-Assessment_Tool.html) is available. NIST SP 800-53A provides guidance for assessing security controls initially selected from NIST SP 800-53 to ensure they are implemented correctly, operating as intended, and providing the desired outcome with respect to meeting the security requirements of the system. Appendix I of NIST SP 800-53 is a supplemental guide addressing ICS. Gaps: No single tool has been defined by the sector to assist asset owners is performing an ICS security assessment. The set of asset owners that will be measured and how they will be measured must also be defined. The initial group could be members of the SCC (18 Chemical Sector trade associations) with target goals of 50% in 2010 and 90% by 2011.
	1.4	Real-time security state monitors for new and legacy systems are in use.	2012	Objective: Provide a parameter that monitors the state of security; the value might range from 0 (no protection) to 100% (all known and applicable standards and practices installed and functioning). Existing Capabilities: There are a number of vendors that provide real-time security state monitors, not necessarily for ICS. Gaps: Definition of real-time. Security state sampling frequency. Definition of the depth of the security state being monitored. Definition of "are in use."

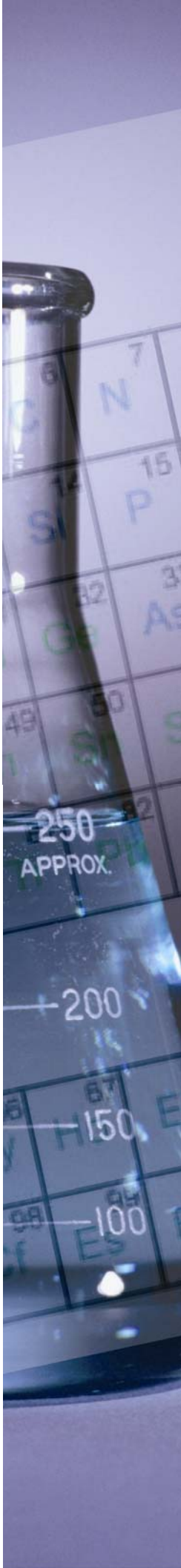


Table D-1. (continued)

Goal	No.	Milestone	Date	Commentary
Measure and assess security posture (continued)	1.5	Fully automated security state methodologies are in use.	2017	Objective: Provide normally hands-off monitoring and implementation of the ICS cybersecurity state. Existing Capabilities: Do not exist. Gaps: The term fully automated security state must be defined. Then the capability must be detailed and developed based on the definition.
Develop and integrate protective measures	2.1	Sector is participating in security training to available, qualified, and consistent control system security training materials.	2009	Objective: Improve the capability of ICS operators to seek, requisition, install, and use adequate security with their ICS. Existing Capabilities: Free training is available from the CSSP, including web-based and instructor-lead training sessions. Training material has been prepared by the CSSP and others. Gaps: Specific sector training objectives have not been established and there are a limited number of qualified trainers. Evolving cyber threats, security requirements, standards, and equipment will require continuous improvements to training materials and techniques.
	2.2	Secure connectivity between business systems and ICS within corporate networks.	2009	Objective: Restrict the highest probable attack path to ICS. In the recent past, cyber attacks on ICS have most often been initated through the internet to the business system and then to the ICS. Business systems have greater need to be connected to the internet. Existing Capabilities: Adequate and acceptable firewalls and/or other isolation methods exist. Gaps: Proper implementation and maintenance.
	2.3	Widespread implementation of methods for secure communication between remote access devices and control centers that are scalable and cost effective to deploy.	2010	Objective: Deter cyber attacks from remote location via legitimate and surreptitious access points. Remote access includes wireless communication devices that have access to the control system. It includes personal communication devices and system state sensors, senders, and receivers. It includes virtual private network (VPN) connections. It includes authorized vendor and system support access. Existing Capabilities: NIST publications such as the 2008 Draft Electronic Authentication Guideline (SP 800-63, Revision 1, December 2008); SP 800-63 Version 1.0.2, April 2006; and Electronic Authentication Guideline (SP 800-63,V1). Also, passwords practices, encryption, firewalls, and verification procedures exist. Gaps: Understanding the ICS security risk with evolving threats and vulnerabilities. Data transmission rate requirements may limit acceptable security measures.
	2.4	Perform nondisruptive intrusion tests on ICS to demonstrate the effectiveness of automated isolation and response.	2011	Objective: Verify the security of a system against access and compromise, the principal vulnerability of cyber systems using nondisruptive intrusion tests. Testing is a time-honored method of verifying the quality and effectiveness of a system. Existing Capabilities: Vendors are available to provide this type of service to the private sector. Red-teams have been used widely. Organizations have a variety of automated intrusion testing platforms to assist in meeting this milestone. Gaps: Lack of confidence and proof that an intrusion test can be conducted without disrupting the operating system and ICS environment. The Chemical Sector has concerns about automated processes on systems that require and include safety integrated systems. Must be conditioned on the type of plant that is being tested. The test will be purposefully initiated by knowledgeable and responsible staff and the isolation and response that is being tested will be automatic.

Table D-1. (continued)

Goal	No.	Milestone	Date	Commentary
Develop and integrate protective measures (continued)	2.5	Secure ICS architectures with built-in, end-to-end security are in all critical operating systems.	2018	Objective: Incorporate cybersecurity requirements into the historical approach to design for safety and reliability and then use add-ons to provide security in legacy systems. Existing Capabilities: Extremely limited. The CSSP provides procurement specification language that may be used when purchacing new systems or components, and developing maintenance contracts for exisiting equipment or systems. Gaps: Effectively all existing systems were not designed, built and installed with an end-to-end secure architecture. Asset owners procuring new components and systems should specify built-in security features and protections. Resolution will require first designing systems and components that are secure-by-design and then replacing all critical operating systems or upgrading them to the equivalent level of security.
Detect intrusion and implement response strategies	3.1	Cyber control system security incident handling guidelines, which provide the means to consistently share generic incident, vulnerability, and lessons learned information, are available throughout the sector.	2009	Objective: Share threat and vulnerability information to enable users to obtain a common risk assessment and establish security enhancement by mitigating known vulnerabiilities across the sector. Existing Capabilities: NIST SP800-61 is a computer security incident handling guide. The ICS-CERT and US-CERT secure portals provide a communication system to report and share incident information. The Department of Homeland Security (DHS) Protected Critical Infrastructure Information (PCII) Program is an information-protection program that enhances information sharing between the private sector and government. Gaps: Guidelines on handling incidents, including a secure method to communicate security incident information—what happened, what caused it, and how was it fixed—must be developed. Currenlty, there is a limited trusted community that provides a virtual forum through which information can be securely shared as needed.
	3.2	Cyber incident response and recovery procedures are included in emergency response plans.	2013	Objective: Integrate cyber risk into corporate cultures. Include cybersecurity in emergency response and preparedness rather than handling cyber attacks separately. Existing Capabilities: The capability presently exists. Suitable cyber incident response is defined and outlined in NIST Special Publications SP800-35 and SP800-61. Gaps: Corporate culture has dictated that cyber incidents should be handled separately from classical emergency response. In many companies, ICS security is separate from IT security.
	3.3	Cyber security monitors that correlate events across the network are in use.	2010	Objective: Maintain rapid recognition of attacks and system weaknesses. Minimize the element of surprise in cyber vulnerability and attacks. Existing Capabilities: Capabilities to monitor and correlate security events of interest currently exist. Implementation on ICS in a cost efficient manner may not be immediately possible. Gaps: Implementing the required monitors and clearly defining the tracking scope. The scope of this roadmap is ICS and not the business system. However, threats, vulnerabilities, and risk span the entire system so that this milestone implies the interface between the restricted control system and the more extensive network to which it is connected.

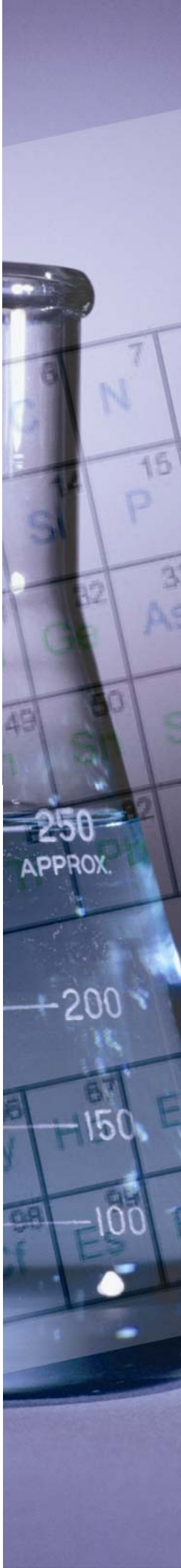


Table D-1. (continued)

Goal	No.	Milestone	Date	Commentary
Detect intrusion and implement response strategies (continued)	3.4	ICS security systems provide contingency and remedial action in response to intrusions and anomalies.	2011	Objective: ICS will be equiped with built-in capability to respond to detect and respond to attacks. Existing Capabilities: None or TBD. Gaps: No generally accepted definition exisits, and further development of these capabilities is required.
	3.5	Self configuring secure ICS network architectures are in use.	2017	Objective: Provide organizations with an automated response capability that includes effective cybersecurity systems. Automatically self-configuring the network architecture would eliminate down time in the event of a partially successful attack. Existing Capabilities: Does not exist. Gaps: Definition and development of these capabilities.
	3.6	Asset owners are utilizing proven industry accepted practices.	2010	Objective: Improved culture of cybersecurity among Critical Infrastructure and Key Resources (CIKR) asset owners where ICS cybersecurity practices are reviewed and implemented. This will provide an effective means of avoiding redundancy and the cost of reinventing solutions. Existing Capabilities: Practices are currently available through the US-CERT website and from industry. The ICS-CERT focuses on situational awareness and recommendations for ICS users. See "Recommended Practices" http://csrp.inl.gov/Recommended_Practices.html and related links. NIST and ISA are both providing and developing ICS standards. Gaps: Current gap is the lack of mature private sector ICS security standards and the insufficeint awareness and implementation.
Sustain security improvements	4.1	Create secure forum for sharing cyber threat and incident response information throughout the Chemical Sector.	2009	Objective: Provide an efficient and effective means of sharing incident data. The sector needs the government to share actionable threat information with the private sector and the private sector needs to report cyber incident information provided to the government. The analyzed incident information needs to be distributed in a timely manner to all industries stakeholders in a efficient manner. Possible working models might be airline incident information shared throughout the industry and nuclear power plant incident information shared with other nuclear power plants. Existing Capabilities: NIST SP 800-61 is the computer security incident handling guide. The ICS-CERT and US-CERT secure portal provides a communication system to report and share incident information. The DHS PCII Program is an information-protection program that enhances information sharing between the private sector and the government. Gaps: Two-way information sharing is needed. The biggest challenge is lack of industry trust and confidence that the shared information will not be misused. CIKR asset owners should share system vulnerabilities discovered during an internal incident response, but not necessarily the details of the incident. Development of guidelines on handling incidents, including a secure method to communicate security incident information: what happened, what caused it, and how was the incident mitigated. Need a trusted community virtual forum through which to share this information.

Table D-1. (continued)

Goal	No.	Milestone	Date	Commentary
Sustain security improvements (continued)	4.2	Undergraduate curricula are available and taught at academic institutions in control system security; scholarships, internships, and research grants are also available.	2010	Objective: Give future ICS engineers an opportunity to take courses with an emphasis on control system cybersecurity. Programs, or even degrees in cyber control system security increase the opportunity for technological improvements in the next generation of secure ICS. Existing Capabilities: There are academic programs for cybersecurity of information technology. The DHS sponsored the development of curricula for a single cyber control system security course in 2006. Gaps: Support for this is not widespread. Control system cybersecurity may be too small a portion in overall control system education. This milestone could be met by integrating cyber control system security into IT security or ICS engineering curricula and programs.
	4.3	Ensure that progress on security improvement efforts presented in this roadmap is periodically shared with the Chemical Sector at various sector events.	2009	Objective: Improve awareness to current events and progress on the improvement of the Chemical Sector's security posture. Track roadmap progress. Improve motivation to further enhance cyber ICS security. Existing Capabilities: Some reporting occurs at annual association events within the sector. Gaps: Gaining access to progress information and providing venues for dissemination.
	4.4	Develop compelling evidence-based business case to explain the cost-efficient investment in ICS security.	2010	Objective: Provide quantitative risk basis for investment in cyber control system security. The lack of investment in cybersecurity is the direct lack of the ability to understand the risk of attack in quantitative (dollars and human impact) terms. Existing Capabilities: Historical tracking such as the Computer Security Institute (CSI) Computer Crime & Security. Survey (http://www.gocsi.com/), the former British Columbia Institute of Technology (BCIT) Industrial Security Incident Database (ISID), Federal Bureau of Investigation (FBI) Computer Crime, a recent survey by Purdue (http://www.forbes.com/), and the ICS/US-CERT incident reporting center provides an estimate of what the risk was, but in an evolving system like cyber ICS, the greatest concern for CIKR is what could, but has not yet happened. Gaps: No quantitative risk analysis approach to the business case exists. This refers to "quantification of risk." Insurance works, generally based on actuarial data from prior experience. Quantification of cyber ICS risk requires quantifying threat and vulnerability and understanding the damage that could potentially occur in attacks ranging from inconvenience to worst-case, catastrophic damage.
	4.5	Integrate cybersecurity awareness, education, and outreach programs into the Chemical Sector.	2010	Objective: Change the culture so that instead of treating "cyber" as a unknown world of its own it is seen as an normal part the industry and the corporation, it is just another parameter that has safety, reliability, security, cost, and value. In particular, cyber risk of ICS, (threat, vulnerability, accepted practices, and requirements to reduce risk) into the corporate and industrial culture similar to the way fire safety is currently handled. Existing Capabilities: All necessary capabilities exist. Gaps: Return on Investment (ROI) for ICS cybersecurity is difficult to obtain and is treated separately from other IT cybersecurity issues. ICS security is viewed as unique due to limited insight from security professionals on how to staff, query, audit, investigate, start, stop, or mitigate based on standard operating practices.

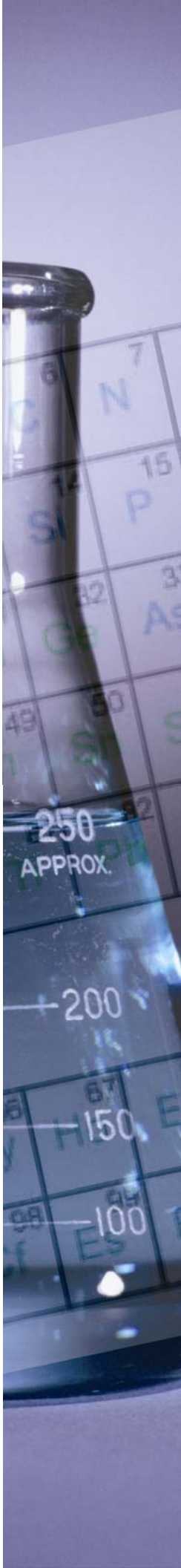
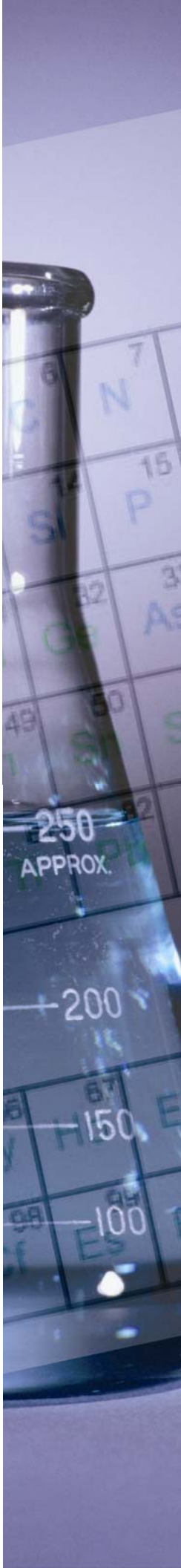


Table D-1. (continued)

Goal	No.	Milestone	Date	Commentary
Sustain security improvements (continued)	4.6	Obtain meaningful incentives through Federal and State government to accelerate investment in secure ICS technologies and practices.	2011	Objective: Seek economic assistance to smaller or highly specialized companies to invest in cybersecurity. Because of the interdependencies of critical infrastructure and the potential for cyber attacks, the cost to protect interconnected orgainzations (or infrastructures) is important and may be beyond the capabilities of a single orgainzation in maintaining their cost competiveness. Existing Capabilities: There is no current capability in this area. Gaps: This was identified as an *Energy Sector Roadmap* milestone and is being supported by the Chemical Sector. In October 2008, the ISAlliance (International Security Alliance) Cyber Policy Recommendations made a strong request for government incentives (tax incentives, government supported test centers, government developed software, etc.) to solve a critical infrastructure problem in a policy paper to the President of the United States. The Defense Industrial Base was the strongest proponent of this.
Secure-by-design	5.1	Owner/operators specify secure-by-design when procuring new cyber ICS.	2010	Objective: Motivate ICS vendors to provide secure-by-design systems and components. Existing Capabilities: DHS has sponsored a program to develop procurement recommendations that will assist in specifying secure-by-design. DHS has published the the "Cyber Security Procurement Language for Control Systems" (ISA-99.04), and "Specific Security Requirements for Manufacturing and Control Systems" which is planned, but not yet drafted, will also provide design requirements. Gaps: CIKR asset owners using these standards to specify new systems and improvements to legacy systems.
	5.2	Commercial products are available that correlate events across the network.	2009	Objective: Provide automated systems that analyze the network traffic for potential attack signatures or nefarious activities. Existing Capabilities: There are a number of vendors that provide real-time security state monitors, but not necessarily for ICS. Gaps: Systems currently available may not be functional in ICS.
	5.3	Owner/operators collaborate with vendors on system and component security improvements.	2009	Objective: Enable vendors to meet the unique control system cybersecurity requirements of owner/operators. Existing Capabilities: System vendors include control system, communications, internet, wireless senders/receivers, software vendors, etc. Collaboration occurs during design and procurement and after installation. Some collaboration is occurring at present. Gaps: The extent to which collaboration is occurring.
	5.4	Real-time security state monitors for new and legacy systems are commercially available.	2011	Objective: Provide a parameter that monitors the state of security; the value might range from 0 (no protection) to 100% (all known and applicable cybersecurity standards and practices installed and functioning correctly). Real-time security state monitor means that it is part of the control system that periodically test and validates that the required security functions are present and functioning. Real-time could mean that test frequency ranges from weekly to seconds, depending on the technical requirements. An example of security functions are provided in NIST SP 800-53A. Existing Capabilities: Security state monitors are currently available for monitoring the state of virus and malware security. Gaps: Definition and agreement of "real-time" functional-full-spectrum security monitors for ICS.

Table D-1. (continued)

Goal	No.	Milestone	Date	Commentary
Secure-by-design (continued)	5.5	A certification center with the capability to verify that cyber ICS and components are secure is available.	2016	Objective: Certify that ICS systems and components meet the specified or designed level of cybersecurity. Owner/operators need to know with a predetermined degree of certainty that the systems they design, buy, install, and operate are secure. Existing Capabilities: Currently, many asset owners utilize test systems to test patches and upgrades before implementation; several commercial entities provide component test systems. Public Law 110-53 (PL-110-53) "Implementing Recommendations of the 9/11 Commission Act of 2007," provides for implementation of recommendations of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) and includes the basis for a Voluntary Private Sector Preparedness Accreditation and Certification Program. Although it seems targeted towards certification of disaster response preparedness, it is not clearly stated. It seems that in the case of cybersecurity, an "all hazards" preparedness would include being prepared to prevent the disaster, which is the implied vision of the roadmap. Thus the certification of the systems as being prepared to deter and prevent the attack from being successful can be implied by the terminology used in this law. Gaps: A sector acknowledged certification program to gage the adequacy of cybersecurity measures within a component or vendor system.
	5.6	Features are available that provide for fully automated security state and common response ICS networks.	2015	Objective: Respond to attacks by first terminating the attack and then adjusting the ICS security state to mitigate the attack and prevent a repeat attack. This needs to be done automatically at a speed that prevents serious physical and economic impact to the industrial process. Existing Capabilities: Some systems currently exist that can terminate known attack types once they have been observed. Gaps: Develop automated security response systems.
	5.7	All COTS (commercial-off-the-shelf) cyber ICS and stand-alone components are secure-by-design.	2015	Objective: Provide systems and components that are secure-by-design. Existing Capabilities: Most systems are designed for production functions and then security systems are added on. Vulnerabilities are identified after the system is in use and patches are provided by the vendor and applied. Gaps: Develop systems and components that are secure-by-design and are certified against a standard. *Legacy systems will remain outside of this goal.*
	5.8	Secure ICS architectures are designed, installed, and maintained with built-in, end-to-end security.	2015	Objective: Provide entire system architectures that are secure-by-design. Existing Capabilities: Does not exist, however, industry agencies are developing an architectural model for consideration. Gaps: Develop standards and designs that implement security features in ICS architectures and topologies.



CHEMICAL SECTOR MILESTONES COMPARED WITH ENERGY SECTOR MILESTONES

Table D-2 lists the *Energy Sector Roadmap* milestones alongside the Chemical Sector Roadmap milestones. The dates in the Date column are anticipated completion dates. Changes, if any, are noted immediately following the *Energy Sector Roadmap* milestone such as "- Modified."

Since this roadmap has added Goal 5, Secure-by-design, which is not included in the *Energy Sector Roadmap*, all milestones directed towards the availability of technological improvements were moved under Goal 5. Furthermore, to achieve the vision, any useful technological improvements called for under Goal 5 must be implemented; therefore a corresponding implementation milestone has been included under Goal 2 or Goal 3. In some cases, the Energy Sector Roadmap identified a milestone directed towards implementing a new technology that was not identified as being developed. In these cases, the Chemical Sector Roadmap includes a corresponding milestone under Goal 5 to provide that technology. These items are summarized below:

- Both Roadmaps have 30 milestones.
- Six of the milestones are identical.
- Five of the *Energy Sector Roadmap* milestones were deleted and combined with another milestone to make a single new milestone for the Chemical Sector Roadmap capturing the same concept. As a result, nine of the Chemical Sector Roadmap milestones appear to be "new" milestones.
- The other 18 Chemical Sector Roadmap milestones were constructed with minor editing of the corresponding *Energy Sector Roadmap* milestone.
- The last change was to delete the qualification that was used in some Energy Sector Roadmap milestones that the desired objective would be met by a certain percentage. The Chemical Sector Roadmap chose to allow the percentage achievement be established during the implementation and monitoring stage.

Table D-2. Comparison Between the Chemical Sector and Energy Sector Milestones

Order	Chemical Sector Roadmap Milestone	Date	*Energy Sector Roadmap* Milestone	Date
1.1	Establish an industry-driven awareness effort to communicate information relating to the cybersecurity threats, vulnerabilities, and risks and the availability of industry accepted practices, tools, and training materials to the Chemical Sector.	2009	Baseline security methodologies available, self-assessments published, and training provided. [Modified]	2006
1.2	Metrics for benchmarking security posture are available and agreed upon.	2010	Common metrics available for benchmarking security posture (relative to peers). [Modified]	2008
1.3	Asset owners and operators are performing self-assessments of their ICS using consistent criteria.	2012	50% of asset owners and operators performing self-assessments of their SCADA using consistent criteria. [Modified]	2008
1.4	Real-time security state monitors for new and legacy systems are in use.	2012	A real-time security state monitor for new and legacy systems commercially available. [Modified]	2011
1.5	Fully automated security state methodologies are in use.	2017	Fully automated security state and common response of control system networks. [Modified]	2015
1.6			90% of energy sector asset owners conducting internal compliance audits. [Deleted, combined with M1.3]	2009
2.1	Sector is participating in security training to available, qualified and consistent control system security training materials.	2009	Publish consistent training materials on cyber and physical security for SCADA widely available within the energy sector. [Modified]	2006
2.2	Secure connectivity between business systems and ICS within corporate networks.	2009	Secure connectivity between business systems and SCADA within corporate network.	2009
2.3	Widespread implementation of methods for secure communication between remote access devices and control centers that are scalable and cost effective to deploy.	2010	Widespread implementation of methods for secure communication between remote access devices and control centers that are scalable and cost effective to deploy.	2010
2.4	Perform nondisruptive intrusion tests on ICS to demonstrate the effectiveness of automated isolation and response.	2011	Perform nondisruptive intrusion, isolation, and automated response exercises at 50% of SCADA.	2011
2.5	Secure control system architectures with built-in, end-to-end security are in all critical operating systems.	2015	Secure control system architectures produced with built-in, end-to-end security. [Modified]	2015
2.6			Make available and disseminate field-proven industry accepted practices for control system security. Deleted, split combined with M1.1 (Make available) and M3.6 (in use)	2008
2.7			Make available security test harness for evaluating next generation architectures and individual components. Deleted, moved the idea to M5.6	2014

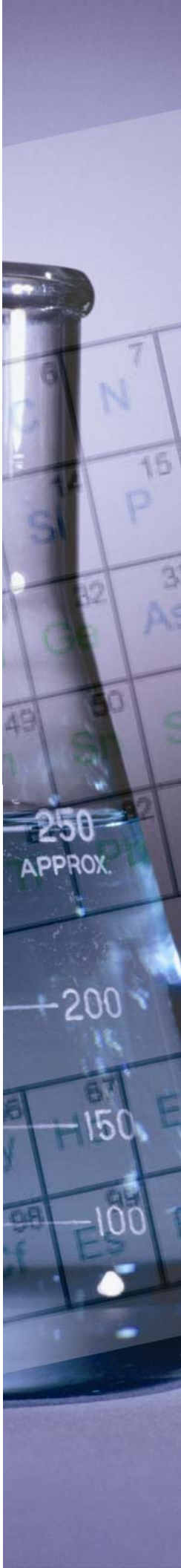
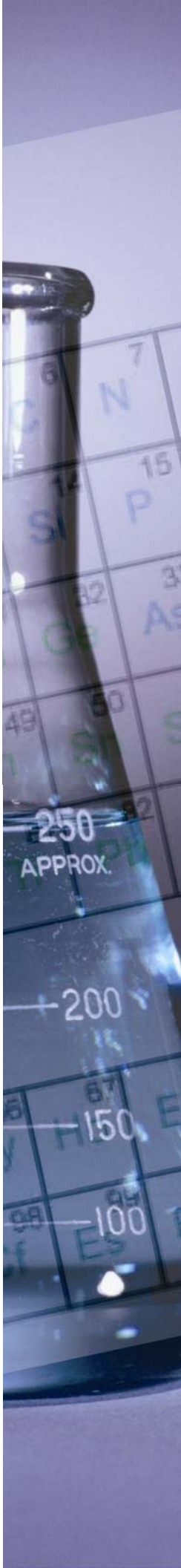


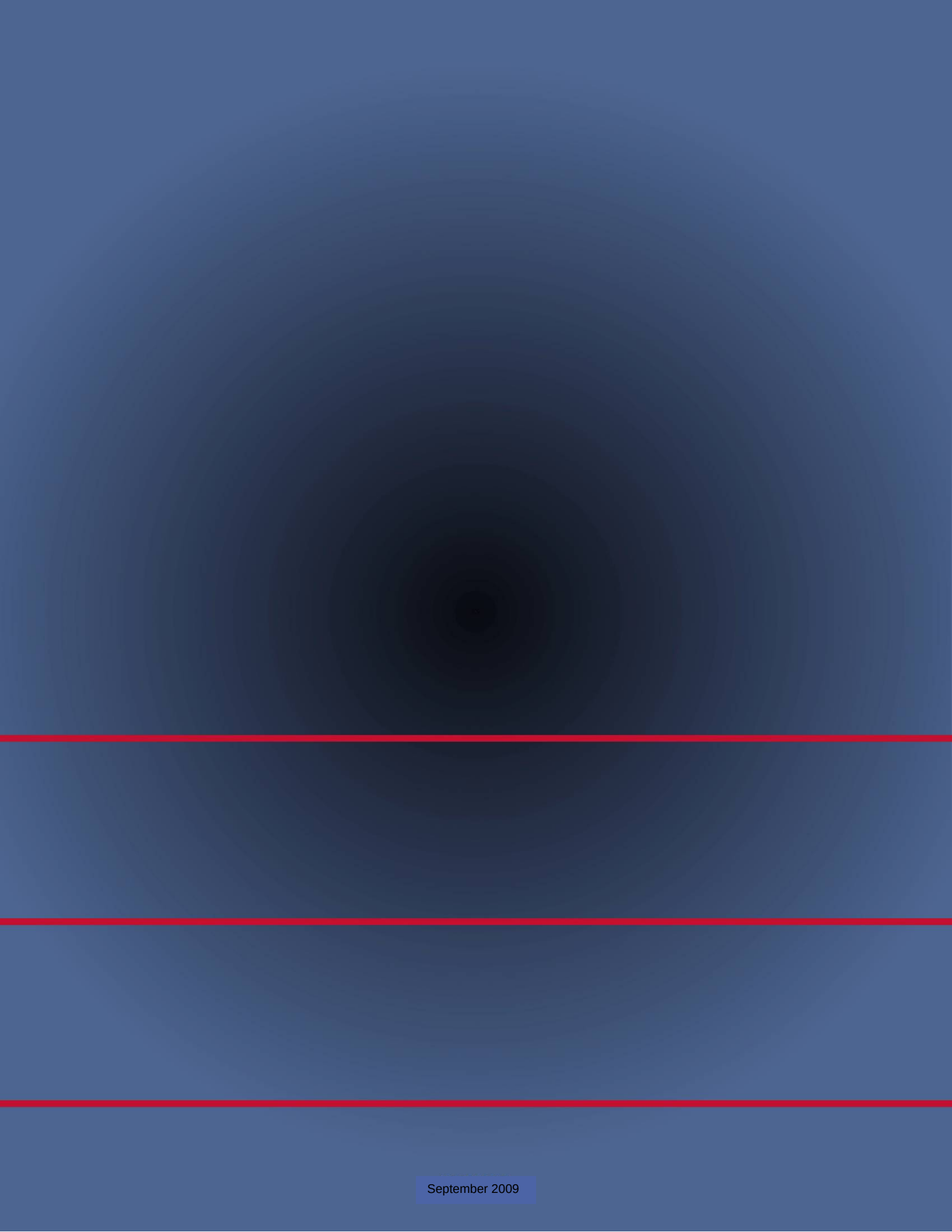
Table D-2. (continued).

Order	Chemical Sector Roadmap Milestone	Date	*Energy Sector Roadmap* Milestone	Date
3.1	Cyber control system security incident handling guidelines that provide the means to consistently share generic incident, vulnerability, and lessons learned information are available throughout the sector.	2009	Incident reporting guidelines are published and available throughout the energy sector. [Modified]	2006
3.2	Cyber incident response and recovery procedures are included in emergency response plans.	2013	Cyber incident response is part of emergency operating plans at 30% of SCADA. [Modified]	2008
3.3	Cyber security monitors that correlate events across the network are in use.	2010	Commercial products in production that correlate all events across the business network. [Modified]	2008
3.4	Control system security systems provide contingency and remedial action in response to intrusions and anomalies.	2011	Control system network models provide contingency and remedial action in response to intrusions and anomalies.	2011
3.5	Self configuring secure ICS network architectures are in use.	2017	Self-configuring SCADA network architectures are in production. [Modified]	2015
3.6	Asset owners are utilizing proven industry accepted practices.	2010	New	
4.1	Create secure forum for sharing cyber threat and incident response information throughout the Chemical Sector.	2009	Create secure forum for sharing cyber threat and response information throughout the energy sector. [Modified]	2007
4.2	Undergraduate curricula are available and taught at academic institutions in control system security; scholarships, internships, and research grants are also available.	2009	Offer undergraduate curriculums in academic institutions in control system security, including scholarships, internships, and research grants. [Modified]	2009
4.3	Ensure that progress on security improvement efforts presented in this roadmap is periodically shared with the Chemical Sector at various sector events.	2009	New	
4.4	Develop a compelling evidence-based business case to justify cost efficient investment in ICS security.	2010	Develop compelling evidence-based business case to increase private investment in control system security.	2007
4.5	Integrate cybersecurity awareness, education, and outreach programs into the Chemical Sector.	2010	Integrate cybersecurity awareness, education, and outreach programs into energy sector operations. [Modified]	2010
4.6	Implement meaningful incentives through Federal and State government to accelerate investment in secure ICS technologies and practices.	2011	Implement meaningful incentives through Federal and State government to accelerate investment in secure SCADA technologies and practices.	2009
4.7			Resolve major info protection and sharing issues between the U.S. government and industry. Deleted, combined with M4.1.	2006

Table D-2. (continued).

Order	Chemical Sector Roadmap Milestone	Date	*Energy Sector Roadmap* Milestone	Date
4.8			Launch industry-driven awareness campaign. Deleted and combined with M1.1.	2006
5.1	Owner/operators specify secure-by-design when procuring new cyber ICS.	2010	New	
5.2	Commercial products are available that correlate events across the network.	2009	New	
5.3	Owner/operators collaborate with vendors on system and component security improvements.	2009	New	
5.4	Real-time security state monitors for new and legacy systems are commercially available.	2011	New	
5.5	A certification center with the capability to verify that cyber vulnerabilities for ICS and components are secure and available.	2016	New	
5.6	Features are available that provide for fully automated security state and common response ICS networks.	2015	New	
5.7	All COTS (commercial-off-the-shelf) cyber ICS and stand-alone components are secure-by-design.	2015	New	
5.8	Secure ICS architectures are designed, installed, and maintained with built-in, end-to-end security.	2018	New	





September 2009