THE NIAC
CONVERGENCE OF PHYSICAL AND CYBER TECHNOLOGIES AND RELATED SECURITY MANAGEMENT CHALLENGES WORKING GROUP

FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL

JANUARY 16, 2007

MARGARET E. GRAYSON
WORKING GROUP CO-CHAIR
PRESIDENT
GRAYSON AND ASSOCIATES

GREGORY PETERS
WORKING GROUP CO-CHAIR
MANAGING PARTNER
COLLECTIVE IQ

GEORGE CONRADES
WORKING GROUP CO-CHAIR
EXECUTIVE CHAIRMAN
AKAMAI TECHNOLOGIES

TABLE OF CONTENTS

I. ACKNOWLEDGEMENTS **.....1**

Working Group Members: 1
Study Group Members: 1

II. EXECUTIVE SUMMARY **.....2**

FINDINGS AND RECOMMENDATIONS 3

III. BACKGROUND ON THE NIAC **.....7**

A. BACKGROUND ON PHYSICAL/CYBER CONVERGENCE WORKING GROUP 7
B. APPROACH 8

IV. BACKGROUND ON THE CYBER THREAT TO SCADA AND PROCESS CONTROL SYSTEMS **.....9**

CONVERGENCE 9
Consequences of convergence 10
THE CYBER THREAT TO CONTROL SYSTEMS 12
CHALLENGES 14

V. FINDINGS AND RECOMMENDATIONS: **.....16**

A. SECURITY AS AN ENABLER 16
Recommendations for Security as an Enabler 18
B. MARKET DRIVERS 18
Recommendations for Market Drivers 20
C. EXECUTIVE LEADERSHIP AWARENESS 21
Recommendations for Executive Leadership Awareness 22
D. GOVERNMENT LEADERSHIP PRIORITIES 23
Recommendations for Government Leadership Priorities 24
E. INFORMATION SHARING 24
Recommendations for Information Sharing 26

VI. CONCLUSION **.....28**

APPENDIX A: FRAMEWORK FOR EXECUTIVE OUTREACH **.....29**

APPENDIX B: NATIONAL INFRASTRUCTURE ADVISORY COUNCIL MEMBERS **.....32**

APPENDIX C: RESOURCES **.....33**

APPENDIX D: THE CURRENT STATE OF SECTOR AND FEDERAL EFFORTS TO ADDRESS CONTROL SYSTEMS SECURITY **.....36**

I. ACKNOWLEDGEMENTS

Working Group Members:

Erle A. Nye, Chairman, Emeritus, TXU Corp., NIAC Chairman
George Conrades, Executive Chairman, Akamai Technologies
Margaret Grayson, President, Grayson & Associates
Gregory Peters, Managing Partner, Collective IQ

Study Group Members:

David Frigeri, Internap Network Services – Study Group Chair (until July 2006)
Page Clark, El Paso Corporation – Study Group Chair
Scott Borg, U.S. Cyber Consequences Unit
Andy Ellis, Akamai Technologies
Rick Holmes, Union Pacific Corporation
Bruce Larson, American Water
Deb Miller, webMethods
Bill Muston, TXU Corporation
John Puckett, DuPont Corporation
Gary Sevounts, Symantec Corporation
Ken Watson, Cisco Systems

Department of Homeland Security (DHS) Resources:

Infrastructure Partnerships Division (IPD)
Nancy J. Wong
Jenny Menna
William Corcoran (contractor)
Eric Hanson (contractor)
Michael Jacobs (contractor)
Gail Kaufman (contractor)
Michael Schelble (contractor)

National Cyber Security Division (NCSD)
Annabelle Lee
Thomas Peters (CSSP)
Jason Phillips (CSSP)
Julio Rodriguez (CSSP - contractor)

II. EXECUTIVE SUMMARY

Charter

Through DHS and the Secretary of the Department of Homeland Security, the NIAC provides the President with advice on the security of the critical infrastructure sectors and their information systems. These critical infrastructures support vital sectors of the economy, including banking and finance, transportation, energy, manufacturing, and emergency government services, among others.

The NIAC convened the Physical/Cyber Convergence Working Group (CWG), in October 2005, to investigate the ongoing convergence of physical and cyber technologies for Supervisory Control and Data Acquisition (SCADA) and process control systems and their consolidated network management. The Working Group convened a Study Group of subject matter experts to inform its work. The Working Group report informed the NIAC's deliberations.

Background

In this report, the term "control system" is used to describe SCADA, as well as industrial, manufacturing, distribution, and process control systems. Different industries and operators use a variety of different terms to describe the systems that run their operations, but all of these systems have the common elements of physical processes and systems that are computer-interfaced and controlled. Control systems operate the physical infrastructures that distribute critical infrastructure services to the public and to other infrastructure operators. The electrical grid and water distribution systems that provide water and electricity to our homes and businesses are examples of vital SCADA systems. Other control systems operate processes to manufacture food or chemical products, and monitor and control natural gas pipelines and petroleum refineries. A cyber attack on these systems has the potential to cause large scale interruption of these services with cascading effects into other sectors of the economy.

The term *convergence* refers to the recent interconnection of Information Technology (IT) systems with these control systems.[1] Until recently, the IT networks that carried business systems were not physically connected to control systems networks and the two systems did not communicate. For a variety of reasons, in recent years, more and more companies have created connections to their control systems, but operators are often unaware of exposure created by these connections. The growing connectivity of control systems is creating new avenues of access for potential cyber attackers. Strategic planning and coordination between public and private sector infrastructure protection partners is vitally needed to adequately address the risk created by the convergence of control systems and IT systems.

Goal

The Working Group focused its efforts on identifying areas of potential vulnerability in Supervisory Control and Data Acquisition (SCADA) and process control system environments and on developing policy recommendations that would enable the effective public-private partnerships necessary to address the cyber threat and to improve the infrastructure protection profile of these critical infrastructure systems.

[1] The Convergence topic was defined in the NIAC study question presented to the group in October 2005.

Scope

This NIAC study examined existing efforts to benchmark this problem and considered numerous available models of infrastructure protection. The study's preliminary findings highlighted the changing environment brought about by the convergence of control systems and IT systems, leading the NIAC to identify ways that current security practices can be strengthened through policy recommendations. This study is limited to the SCADA and process control system environments that are prevalent throughout many of the critical infrastructure sectors. Other intersections of cyber and physical technologies, such as building automation, were deemed out of scope for this study.

Approach

The Working Group identified five key questions to study for potential improvement in public-private partnership and policy. These five questions are:

1. How can security be positioned as an enabler of the established goals of control systems operators?
2. What actions can be taken to improve market drivers for control systems security?
3. How can executive awareness be raised to facilitate a measured and appropriate response in the private sector?
4. What are the appropriate Federal government leadership roles and priorities for achieving control systems cyber security?
5. What policies and mechanisms would facilitate the needed information sharing to improve the cyber security posture of critical infrastructure control systems?

Findings and Recommendations

Security as an Enabler

The NIAC found that to promote a corporate culture where cyber security is valued as an enabler to control system operator goals of availability, reliability, and safety, executive leadership must fully understand the risk to control systems. To achieve this, critical infrastructure protection partners must educate executive leaders regarding the risk to their control systems and build the information sharing mechanisms needed to increase understanding of the risk.

The NIAC recommends:

1. The President establish a goal for all critical infrastructure sectors that no later than 2015, control systems for critical applications will be designed, installed, operated and maintained to survive an intentional cyber assault with no loss of critical function.
2. The Department of Homeland Security (DHS) and Sector-Specific Agencies (SSAs)[2] collaborate with their respective owner/operator sector partners to develop sector-specific roadmaps using the Energy Sector Roadmap as a model.

[2] Sector-Specific Agencies (SSAs) are the Federal departments and agencies identified in Homeland Security Presidential Directive 7 (HSPD-7) as responsible for CI/KR protection activities in specified CI/KR sectors. The National Infrastructure Protection Plan (NIPP) assigns a federal agency to act as SSA for each of the 17 CI/KR sectors.

3. DHS promote uniform acceptance across all sectors that investment in control systems cyber security is a priority. For sectors with regulatory oversight of earnings and investments, DHS should promote inclusion of the costs of control systems cyber security as legitimate investments and expenses that deserve approval by their regulatory bodies.
4. DHS and other relevant Federal agencies implement Convergence Study recommendations for Improved Information Sharing.
5. DHS and other relevant Federal agencies implement Convergence Study recommendations for Executive Leadership Awareness and the framework in Appendix A.

Market Drivers

The NIAC found inconsistent market drivers across the sectors to develop and implement secure products and systems because the control systems market is in the early stages of a transition. Awareness of the security issues and needs is uneven across the critical infrastructure sectors, and the cost of developing and implementing security features is prohibitive for many operators and vendors.

The NIAC recommends:

1. The Office of Management and Budget (OMB) mandate that Federal agencies apply the *Cyber Security Procurement Language for Control Systems*[3] document and existing security and security-relevant standards and criteria when procuring control systems and services.
2. DHS and the SSAs encourage the application of existing security and security-relevant standards and criteria in developing and implementing secure control systems.
3. DHS and the SSAs encourage owners and operators to identify and utilize existing security and security-relevant standards and criteria for their control systems. The process of applying these standards and criteria will provide the basis for continuing development of each operator's requirements to achieve control systems security.
4. The Sector Coordinating Councils (SCCs) apply the sector self-governance approach outlined in the framework of the NIAC's *Best Practices for Government to Enhance Security of the National Critical Infrastructures*, April 2004, with validation by the SSA for evaluation of self-governance effectiveness within each sector and as an educational tool to establish reasonable sector steps to improve self-governance.

Executive Leadership Awareness

The NIAC found that executive leadership awareness of the cyber threat to control systems, within government and industry operators and vendors, is critical to achieving all needed actions.

The NIAC recommends:

DHS work with SSAs to implement a program for control systems cyber security executive awareness outreach. This outreach will include the elements outlined in the attached Framework in Appendix A. Key elements of the outreach program include:

- Value for senior executive-level decision maker participants through inclusion of relevant strategic threat information gathered by the Intelligence Community.

[3] Document available at: http://www.msisac.org/scada/

- Establishment of a continuing dialog among parties relevant to critical infrastructure control systems in the public- and private-sectors, owner-operators and supporting government agencies, and vendors involved in control system implementations, including IT and Security.
- A protected forum for discussion of strategic information through use of the Critical Infrastructure Partnership Advisory Council (CIPAC)[4] framework and SCCs.
- Awareness outreach to address executive-level decision makers in critical infrastructures, as well as owner-operators and relevant decision makers in SSAs, State, and local government.
- Strategic-level conversations to achieve operator vulnerability self-discovery, making use of strategic-level information on threats, hostile actors, economic motivators for hostile actors, and economic and physical consequences.
- DHS promotion of critical infrastructure control systems vulnerability assessments for development of corporate awareness.
- Education of executives that control systems cyber security is critical to the corporate goal of operational safety.

Government Leadership Priorities

The NIAC found strong and committed government efforts underway to address the cyber threat to control systems. Government actions could benefit from private-sector feedback and from higher-level interagency coordination and strategic planning to best address the cyber threat to control systems.

The NIAC recommends:

1. SSAs assign a senior executive leader, at the Assistant Secretary level, as responsible and accountable for their agency's collaboration with DHS efforts to address control systems cyber security for their sector. This group should meet annually with the Partnership for Critical Infrastructure Security (PCIS)[5] to evaluate each sector's strategy to meet the national control system survivability goal set for 2015, outlined in the recommendations for "Security as an Enabler" section above.
2. The Federal government incorporate private-sector input into the cyber research and development (R&D) funding prioritization processes conducted by the Office of Science and Technology Policy (OSTP) and Office of Management and Budget (OMB). Sector Specific Plans (SSPs) will provide initial input and SSAs will establish additional avenues for their sectors in the future.
3. DHS work with the Malcolm Baldridge Award for Excellence in Business Management and/or other similar programs to help communicate the importance of control systems cyber security to business leaders.

Information Sharing

[4] The CIPAC structure was recommended by the NIAC as a result of the Sector Partnership Working Group Study and formally created by Homeland Security Secretary Chertoff in March, 2006.

[5] Created in 2001, PCIS is a privately incorporated organization that draws membership from each of the CI/KR Sector Coordinating Councils (SCCs). PCIS was formally recognized by the 2006 National Infrastructure Protection Plan (NIPP) for their role in public-private partnership for infrastructure protection issues.

The Council found that improved sharing of information on control systems threats, vulnerabilities, consequences, and solutions is vital to a properly informed and measured response to the threat to critical infrastructure control systems.

The NIAC recommends:

1. DHS enhance the control system cyber incident information collection mechanism at Carnegie Mellon's CERT Coordination Center (CERT/CC) for comprehensive collection, protection, and sharing.
2. DHS rapidly ramp up CERT/CC's support services for control system operators to help develop a cyber incident information collection capability.
3. The Office of the Director of National Intelligence (DNI)[6] develop a solution to the problem of originator control (ORCON) that currently prevents DHS from sharing threat information with critical infrastructure operators.
4. The Intelligence Community produce a Threat Assessment followed by a National Intelligence Estimate (NIE) for control systems threats to begin the process of establishing a knowledge base.
5. DHS share relevant information from the Threat Assessment and NIE with critical infrastructure control systems operators.
6. DHS enhance existing program activities to create the ability to integrate and track understanding of the cyber risk for critical infrastructure control systems using all available sources.
    a. This collaborative program should collect, correlate, integrate, and track information on:
        - threats, including adversaries, toolsets, motivations, methods/mechanisms, incidents/actions, and resources;
        - consequences, including potential consequences of compromise to sector, industry, and facility-specific control systems; and
        - vulnerabilities in control systems or their implementations in the IT infrastructure that adversaries could exploit to gain access to critical infrastructure control systems.
    b. This capability is a DHS operations function, and will include input and expertise from: critical infrastructure owner/operators and other relevant parties in the private sector regarding consequences and vulnerabilities, the Intelligence Community on threats, CERT/CC and other sources on incidents, and DHS (including US-CERT) on cyber vulnerabilities.
    c. DHS will communicate resulting warning information to control systems owner-operators to ensure protection of U.S. critical infrastructures.
7. The Program Manager, Information Sharing Environment, include information on control systems cyber threats in the Information Sharing Environment (ISE).

6 The Office of the Director of National Intelligence (DNI) was formed as an outcome of the Intelligence Reform and Terrorism Prevention Act of 2004. The Director of National Intelligence (DNI) serves as the head of the Intelligence Community (IC) and also acts as the principal advisor to the President, the National Security Council, and the Homeland Security Council.

III. BACKGROUND ON THE NIAC

Through DHS and the Secretary of the Department of Homeland Security, the NIAC provides the President with advice on the security of the critical infrastructure sectors and their information systems. These critical infrastructures support vital sectors of the economy, including banking and finance, transportation, energy, manufacturing, and emergency government services, among others.

The NIAC identified that physical infrastructures operated by SCADA and process control systems are becoming vulnerable to cyber attacks. Control systems also present unique technical challenges that distinguish them from general business systems. The consolidation of their network management and increasing connections to corporate business systems and other access points such as wireless technologies, present a new and evolving risk to these critical infrastructures.

The NIAC convened the Physical/Cyber Convergence Working Group (CWG), in October 2005, to investigate the ongoing convergence of physical and cyber technologies. The CWG studied whether the public and private sectors are adequately addressing control system vulnerabilities, and given the ongoing convergence, what actions would be appropriate for government and industry to address this new risk.

The NIAC is charged with:

- enhancing cooperation between the public and private sectors in protecting information systems supporting critical infrastructures in key economic sectors and providing reports on the issue to the President, as appropriate;
- enhancing cooperation between the public and private sectors in protecting critical infrastructure assets in other key economic sectors and providing reports on these issues to the President, as appropriate; and,
- proposing and developing ways to encourage private industry to perform periodic risk assessments of critical information and telecommunications systems.

The NIAC also advises the lead Federal agencies that have critical infrastructure responsibilities and industry sector coordinating mechanisms.

A. *Background on Physical/Cyber Convergence Working Group*

The NIAC asked the Physical/Cyber Convergence Working Group to look at existing work in the control systems environment in terms of standards and best practices, the current state of research, development, and practice, and ongoing government programs. Furthermore, the NIAC asked the Working Group to determine the most appropriate actions for government and industry to achieve needed cyber security for our Nation's critical infrastructure control systems. The Working Group convened a Study Group of subject-matter experts to inform its work.

This report was researched and written to address the cyber security challenges of converged process control/SCADA and IT systems. Although the investigations focused on the Chemical, Energy, Transportation, and Water sectors, this report potentially has implications for each of the seventeen critical infrastructure sectors and key resources (CI/KR) identified in Homeland Security Presidential Directive-7 (HSPD-7),[7] because commonality and convergence exist in all of the sectors to differing degrees.

B. *Approach*

To frame the discussion on control system security, the Working Group began by developing and validating five framework questions that set the scope of the topic for the investigation process. These framework questions are:

1. ***Security as an Enabler*** – What is the best way to position cyber security as a contributor and an enabler to achieving reliability, availability, and safety goals in the management of SCADA and process control systems?

2. ***Market Drivers*** - What are the market drivers required to gain industry attention and commitment to research and product development and implementation?

3. ***Executive Leadership Awareness*** – What policies would best generate executive leadership awareness to assist in creating a culture and environment that values the protection of SCADA and process control systems from cyber threats?

4. ***Federal Government Leadership Priorities*** - What are the appropriate Federal government leadership roles and priorities in identifying threats, vulnerabilities, risks, and solutions?

5. ***Improving Information Sharing*** - What are the obstacles and recommendations for improving information sharing about process control systems and SCADA threats, vulnerabilities, risks, and solutions?

After validating these five questions, the Working Group used them to investigate the topic, first identifying the key elements to each of the questions and then the corresponding desired end states. Finally, the Working Group identified recommendations to achieve the desired end states of each key element and each framework question. Along the way, the Working Group used conversations with subject-matter experts to validate the key elements, end states, and potential recommendations. The process included weekly conference calls with subject matter experts on specific, identified issues and frequent workshop meetings to discuss topics that were more difficult.

[7] HSPD-7 was issued December 17, 2003. Available at: http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

IV. BACKGROUND ON THE CYBER THREAT TO SCADA AND PROCESS CONTROL SYSTEMS

For the purposes of this report, the term "control system" will be used to describe Supervisory Control and Data Acquisition (SCADA), industrial, manufacturing, distribution, and process control systems. While all control systems share the common characteristic of using computers to control physical systems or processes, their configuration, application, and nomenclature can vary widely. SCADA systems are networked systems of geographically distributed devices used to monitor and operate the functions of a production, transportation, or distribution system. The term *process control system* is used often to describe systems confined to a building or facility that run production, distribution, or batch process systems found in medical facilities, refineries, power plants, manufacturing plants, and similar industries.[8] Different industries and operators use a variety of different terms to describe the systems that run their operations, but, no matter than nomenclature or terminology, all of these systems have the common elements of physical processes and systems that are computer-interfaced and controlled.

A control system can include thousands of distributed devices, and some systems have a life cycle of more than 30 years, representing significant capital investment for an operator. These characteristics combine to create systems with extremely high value to their owners, and they also create challenges for implementing network security because the components of these systems are not frequently replaced or upgraded due to cost.

Convergence

For the purposes of this report, the concept of *convergence* refers to the combining of Information Technology (IT) systems with computerized process control systems. Until recently, most control systems were isolated from IT systems with an "air gap" – the IT networks that carried business systems were not physically connected to control systems networks and the two systems did not communicate. As IT technologies have advanced, companies have increasingly sought to monitor and manage the outputs of their production systems and to establish data repositories on production system performance for maintenance planning and performance improvement planning efforts. In doing so, the control systems are becoming interconnected with business systems. Market-driven consolidations in IT vendors and standards have also contributed to this convergence as newer digital control system technologies are moving toward common TCP/IP protocols. Business systems connected to the Internet are exposed routinely to cyber attacks conducted over the Internet. This growing connection of control systems to business systems presents new avenues of access to control systems for potential cyber attackers, as do emerging technologies, such as wireless communications and removable storage devices. The convergence between control systems and IT systems in America's critical infrastructures must be addressed to prevent future cyber attacks with catastrophic consequences, including infrastructure failures.

[8] Brief by Andrew Wright (Cisco Systems Critical Infrastructure Assurance Group) to the Convergence Study Group, January 2006.

Consequences of convergence

This evolution toward network connections between IT and control systems, along with other advances in technology and business practices, has exposed previously isolated control systems to Internet attacks. Other new exposures include unsecured network connections, such as wireless devices, control systems network connections to third party maintenance vendors, and network-outsourced business process connections.

The most immediate consequence of a successful cyber attack on critical infrastructure control systems is a loss of the ability to provide its critical service to society. In addition to the immediate loss of service, penetration of IT systems can cause businesses to lose significant value, including the loss of proprietary intellectual property and processes.

Scott Borg, of the U.S. Cyber Consequences Unit, a non-profit, independent research organization (see Appendix D), believes that a sophisticated and successful attack on a control system can present an entirely different set of consequences with liabilities that could potentially exceed the value of the company and present significant economic consequences to those served by these critical infrastructures.[9]

Another problem caused by the convergence of IT and control systems is that many companies, particularly at the senior management level, are not aware of the new threats and risks to their control systems that result from these changes.[10] This change has not escaped the notice of potential attackers who are now showing an interest in control systems and how to manipulate them, creating a real threat with high impact consequences.[11]

Control systems have not developed in parallel to the rapid and widespread growth of IT systems over the last two decades. Control systems components have substantially different design and operating requirements, and may have significantly longer lifecycles than most traditional IT systems. While businesses have found it financially advantageous to update IT systems every several years to capitalize on advances in computer technology, control systems operators have not. Control systems have different performance characteristics and financial drivers that result in stable long-term use.

The control systems of today do share many commonalities with modern IT systems. Control systems are computer networks with computer interfaces and intelligent devices. Technology is pushing many updated systems from slower serial communications toward the faster, more common digital TCP/IP network communications protocols used by IT systems. Also, there is an emerging trend among newer, lower-end control systems toward the use of common IT operating systems. Increasingly, control systems are networked with a company's business systems to improve monitoring and management

[9] Presentation to the Convergence Study Group by the US-CCU, April 13, 2006, slide 8.

[10] Discussions with DHS and numerous security experts highlighted a repeating pattern of widespread unawareness among operators with regard to their control system's external connections.

[11] The increase in "black hat" hacker interest in control systems manipulation was noted by DHS and included in a presentation by INL to the SANS Security Conference in March, 2006.

of a system's operations, and operators are often unaware of these network connections to their control system.

Despite these obvious commonalities, control systems can differ from most IT systems in very significant ways. Control systems operate around-the-clock to optimize the return on a system's investment or provide high availability services, such as those provided to utility customers. In contrast, most IT systems have structural redundancy or scheduled downtimes that can be used for maintenance and system updates.[12] Unlike IT systems, control systems networks require real-time communication for systems operation and have less tolerance for network failures or latency in communication time.[13] Operating systems software for control systems often include modifications to the standard version software and security patches may require extensive testing and modification from the control system vendor before safe implementation by an operator is possible. IT system downtime allows IT managers to implement, update, test, and refresh systems with new technology. Without this available downtime, control systems operators face significant difficulty implementing simple common IT security practices.

The physical facilities and processes that control systems operate are very diverse, and, as a result, systems are often custom-built – made up of control devices and operating systems available at the time the system was implemented. These older systems are also often patched together with unique device driver code and customized computer code written by the engineers or vendors who installed the system and modified it over the years. As a result, these older legacy systems still use outdated operating systems that meet operational needs but lack current security management. Operators continue to use these older machines and code because of the tremendous value of the systems and the cost required to replace, change, or update them.[14]

Another significant convergence-related problem is that legacy control systems often suffer from poor device coding and configuration practices because of an array of related factors that center on cost-cutting and the limitations of older devices. As a result, buffer overflows and unrecognized device inputs, including system port scans, can knock control system devices offline.[15]

The cultural difference between IT operators and control systems operators is another obstacle to addressing the convergence issue. Historically, control systems and IT systems have operated separately and autonomously. The convergence of these systems is also merging the work of two groups. As a generalization, IT staffs are typically younger with most of their experience coming from running business networks, with relatively limited understanding of control systems and their operational requirements. In

---

[12] First presented to the Convergence Study Group by Bob Mick, of ARC Advisers, December 2006,.
[13] From *Presentation to the Convergence Study Group* by Bob Mick, ARC Advisory Group, December 2006, slide 5.
[14] From *Presentation to the Convergence Study Group* by Bob Mick, ARC Advisory Group, December, 2006, slide 5.
[15] System failures due to poor device coding practices were brought to the group's attention during conversations with Study Group chair and subject matter expert Page Clark.

contrast, control systems operators are engineers, often older than their company's IT staff members, and their experience is often centered on a production system with a relatively limited understanding of IT systems.[16] The operational goals of the two groups are also different – control systems operators strive for availability, reliability, and safety, while IT security practitioners stress confidentiality, integrity, and availability of data.[17] Additionally, there are differences in the language and nomenclature that the two sides use for parallel aspects of their work. Although the language differences are not great, the cyber security risk to control systems resulting from this convergence creates the potential for serious consequences from miscommunication. Successful convergence – securing critical infrastructure control systems from cyber threats – depends on these two groups communicating successfully and understanding each other's concerns, goals, and objectives.

The Cyber Threat to Control Systems

The Working Group received classified briefings on the cyber threat to control systems, spoke with subject matter experts and operators regarding their experiences in the field, and analyzed publicly available information regarding cyber attacks on control systems. The Working Group found that the cyber threat to critical infrastructure control systems is real – it is present today and the frequency and sophistication of these attacks is growing. Although there are no commonly known examples of infrastructure failures that can be tied to a cyber attack, the potential for such an event exists and the consequences could be catastrophic.

One reason companies that operate control systems are failing to address these new vulnerabilities is that decision makers within these companies often have a limited understanding of the threat. When discussing cyber threats and hackers, many control systems operators think only of IT system failures such as emailed viruses, worms, denial-of-service attacks, and novice hackers breaking into systems, purely to see if they can gain access (commonly referred to as "script kiddies"). The emerging cyber threat far exceeds these tactics and hostile actors can include individual criminals, organized crime, rogue corporations, terrorist organizations, and nation states. Each of these different actors brings to bear a wide range of intents, skill levels, motivations, and resources.[18]

The cyber threat to critical infrastructure control systems is only beginning to emerge. Beginning in late 2003 and escalating significantly in 2006, government and non-government organizations monitoring the anti-establishment "black hat" hacker community, report seeing a steady increase in discussions, not just of how to penetrate information systems, but of how to use them to manipulate internal processes to achieve

[16] Concept first discussed by Bill Muston with Andrew Wright and Venkat Pothamsetty of Cisco Systems.
[17] The contrast between IT Information Assurance (IA) attributes and control system operational goals was developed by the Convergence Study Group over the course of several subject matter expert conversations. Some control systems cyber security standards, do, however, continue to stress IA attributes to achieve security.
[18] *US-CCU presentation to the Convergence Study Group*, Scott Borg, April 13, 2006, pp. 3.

specific objectives.[19] As a result of these discussions, an increasing number of hackers have focused their attention on control systems over the last two years. Researchers at the British Columbia Institute of Technology (BCIT) report that they have also observed an increase in the control systems cyber incidents entered into their Cyber Incident Database (CID) during this period. They believe this reflects an increase in the overall frequency and sophistication of such attacks.[20]

Many control system operators falsely believe they can maintain "security through obscurity."[21] Because these operators are utilizing customized, proprietary, or antiquated software, they believe that sabotage to their systems is unlikely, because no one would understand how to manipulate their "obscure" controls, even if their network were to be successfully penetrated. Operators also often believe that their systems' obscurity makes them immune to the distributed Denial of Service (DDOS) attacks and data thefts experienced by IT systems in the business world.[22] This complacency is unjustified and dangerous because control systems are designed to be easy to understand to reduce human operator error and because knowledge of control systems is becoming increasingly diffused and readily available.

Cursory IT security implementations can also create a false sense of security for operators. For instance, control systems operators sometimes place firewalls between their control systems and IT systems. However, firewalls must be configured properly to protect a network, and even then, they are vulnerable to a cyber attack. Another issue for control systems is that the security implementations and practices established for business systems have not been applied to previously isolated control systems networks, and their recent connection to the Internet could render them exposed, without robust IT security practices in place.

The NIAC also found that one of the reasons most infrastructure owners and operators were unaware of this growing cyber threat is that much of the useful government data on cyber attacks is classified. Most control systems operators lack the proper clearance to receive this information, and information sharing between the intelligence community and infrastructure owner-operators is not well developed. Operators have not seen, and therefore do not understand, the threat to their systems.

Operators also often misunderstand the economic consequences of cyber attacks. Most operators believe a cyber attack would involve shutting down their system due to a DDOS attack, leading to a minor disruption of operations. US-CCU research has shown, however, that for most companies with operations-critical control systems, there are other hypothetical cyber attacks that would have much worse effects. Most of these highly destructive cyber-attacks would involve the manipulation of instructions or data, rather

[19] This event was noted by DHS' CSSP and presented to the March 2006 SANS conference by INL.
[20] Discussion with Dr. Eric Byers of BCIT, March 9, 2006.
[21] Discussion with Dartmouth Institute for Security Technology Studies, February 16, 2006.
[22] From discussions with Scott Borg, US-CCU, April 13, 2006.

than simple denials of service. The US-CCU believes many of these attacks could create liabilities large enough to bankrupt the companies in question.[23]

US-CCU research shows some operators also misunderstand or misinterpret the potential motivations of would-be attackers. The common perception is that the only motivation for critical infrastructure cyber attacks is malicious harm, but cyber attacks can also be used by the attacker to achieve a variety of objectives, including, but not limited to, large financial gains, untraceable by law enforcement.[24]

The cyber threat to critical infrastructure control systems is also a global issue. Many companies operating critical infrastructures in the United States are international companies with global operations and global IT networks. Potential hostile actors worldwide can connect to the Internet and attempt to carry out cyber attacks from anywhere in the world. This report focuses on policy recommendations for domestic action, but successful solutions will need to consider the international aspects of the problem, as well. Control systems vendors have international customer bases and, in some cases, are multinational corporations. Because security solutions can involve protected technologies, some technology solutions fall within the limitations of U.S. export control laws, limiting vendor response to customer requests and necessitating prohibitively expensive split product-development lines.

Challenges

Some of the structural challenges to adequate cyber security for critical infrastructure control systems identified by the NIAC include infrastructure dependencies and high cost for smaller, revenue-restricted companies and public utilities. The cost of needed investments has the potential to be very high, even for those companies that can afford it. Smaller companies with restricted revenue and large control system implementations face an enormous potential cost to secure their systems. Many of these companies are critical players in their sector, given that larger infrastructure companies depend upon their operations. Public utilities with large systems and revenue streams restricted by public policy face the prospect of either absorbing increased expenses or making a case for increased investment for expenses associated with security before a utility commission in order to make the formal *rate case* required by law that would generate the revenue for such a large investment.

Like other NIAC Working Groups before it, the Physical/Cyber Convergence Working Group found that there are significant differences among the critical infrastructure sectors. The NIAC found that each infrastructure sector has a very different control systems profile, with varying exposures and vulnerabilities to cyber attack. This eliminates the possibility that one set of security standards or one set of cyber security solutions could be applied across all infrastructure sectors to address the problem. In addition, the NIAC found that each sector has a very different dynamic with regard to cooperation and collaboration. For example, the electric sector has a long history of inter-company cooperation beginning with the establishment of the North American

[23] *US-CCU presentation to the Convergence Study Group*, Scott Borg, April 13, 2006, pp.8.
[24] *US-CCU presentation to the Convergence Study Group*, Scott Borg, April 13, 2006, pp.4.

Electric Reliability Council (NERC) in 1968, whereas other sectors such as the Chemical Sector have a strong tradition of competition and less cooperation.[25] Again, these differences would hamper any attempt to enact a single cross-sector policy to address the problem.[26]

Part of the NIAC's effort included outreach to business leaders active in the effort to understand their concerns. The NIAC discovered that operators gave vendors very low grades on their efforts to introduce security to control systems. Vendors, in turn, gave operators very low marks on their willingness to accept, pay for, and implement security solutions for control systems.

[25] From conversations with Study Group member and subject matter expert John Puckett, Chief Technology Officer for DuPont Corporation.
[26] Conversation with Stan Johnson, North American Electric Reliability Council (NERC), July, 2006.

V. FINDINGS AND RECOMMENDATIONS:

A. *Security as an Enabler*

The NIAC found that to promote a corporate culture where cyber security is valued as a enabler to control system operator goals of availability, reliability, and safety, executive leadership must fully understand the risk to control systems. To achieve this, critical infrastructure protection partners must educate executive leaders regarding the risk to their control systems and build the information sharing mechanisms needed to increase understanding of the risk.

Historically, control systems operators developed and built their systems to achieve primary characteristics of operational availability, reliability, and safety. In the converged control systems of today, cyber security is critical to maintaining these established operational characteristics. Without investment in cyber security, control system operators will be unable to meet their desired levels of availability, reliability, and safety.

Within the industry, the terms availability, reliability, and safety encompass the characteristics that maximize operational efficiency and revenue, while minimizing financial losses. In this context, investment in cyber security is often viewed as an added cost with no discernable improvement in operational efficiency or revenue. In some cases, operators view increased cyber security implementation as a detriment to achieving these desired operational characteristics. The environment in which these systems operate has changed dramatically in recent years. Once isolated from business and other networks, control systems are now networked with the business systems that monitor and manage their output, which, in turn, are connected to the Internet. Maintenance connections to third-party vendors and wireless connections have resulted from changes in business models and technology. Where these connections increase the control system operator's efficiency and reduce costs, they also create potential avenues for cyber attack on a control system. A successful such cyber attack can disrupt the availability, reliability, and safety characteristics of the system, resulting in a significant impact to the company's operational efficiency and revenue. Today, investment in cyber security is essential and can not be separated from the critical control systems operational characteristics of availability, reliability, and safety.

The question remains: how do you communicate to control systems operators the need to invest in security to protect their systems, and what is the appropriate level of investment?

For a typical company, investments in cyber security are considered in the context of risk management Return on Investment (ROI) calculations. For a risk management ROI calculation, the operator needs to be able to determine the probability of an incident, given existing vulnerabilities and cost of the consequences, along with the price of the preventive investment. To make a decision to invest in cyber security, the operator must be able to estimate the probability of a cyber attack as well as the potential consequences.

NIAC investigations found that the volume of data needed to calculate incident probability and the potential revenue implications that would justify appropriate cyber security investment currently does not exist. The emerging, dynamic, and growing nature of the cyber threat further accentuates this problem. One reason the information doesn't exist is that companies have no way of sharing this information safely, and they fear a loss of customer and investor confidence if an incident were to become public.

Upon closer inspection, cyber security investment for control systems does have an identifiable return. The issue exceeds the importance of simple risk assessment ROI decision making. The common corporate hierarchy of decision making goes, in order of importance: safety, regulatory compliance, and then ROI. To achieve appropriate investment for control systems security, the discussion needs to be framed in terms of safety rather than ROI or risk assessment.

Executive leadership awareness is another critical element to investment in control systems cyber security. Executives are responsible for making safety-level investment decisions and they are primarily responsible for establishing their company's corporate culture. The level of investment required to improve control system cyber security often rises above the discretionary-level spending afforded to most control systems operational-level managers; these decisions belong to executive leadership. Executive leaders of control systems vendors, solutions providers, and public- and private-sector critical infrastructures must have awareness and understanding of cyber threats, vulnerabilities, and consequences if they are going to promote the culture needed to view cyber security as a contributing factor to control system availability, reliability, and safety.

Some operators have already identified control systems cyber security as a safety issue due to the potential physical consequences, a core value for most corporations. Study Group conversations with Dr. Eric Byres, founder of the BCIT Industrial Security Incident Database (ISID), showed that major corporations in the Energy sector, when confronted with an undetermined probability of a cyber incident, chose to invest a significant amount of capital to address their control system vulnerabilities, based entirely on the issue of maintaining safety standards.

Improved sharing of cyber incident information for control systems is required to achieve needed critical infrastructure control systems cyber security investment. Currently, most control systems operators have no access to any information on cyber incidents because the needed mechanisms do not exist to adequately protect shared information. The information that does exist in the BCIT database is not accessible to many operators due to safeguards established by BCIT to assure the trust and confidence of the owner-operators sharing information. These safeguards have also limited the scope of the information collected for those owner-operators participating in the database.

Because many control systems operate critical infrastructures, the cyber risk to these systems can produce consequences that far exceed the direct losses of the operating company. Interruption to critical infrastructure services include economic and societal consequences reaching far beyond the company that operates the system. This important

issue needs leadership and planning to be successful in setting and achieving goals for cyber security. The Energy sector has taken steps to address these issues in its *Roadmap to Secure Energy Sector Control Systems for the Future*, which outlines a specific plan to reach the goal of securing systems to survive an intentional cyber attack within the next 10 years.

Recommendations for Security as an Enabler

To promote a culture where security is valued as an enabler to existing control system operational goals, the NIAC recommends:

1. The President establish a goal for all critical infrastructure sectors that no later than 2015, control systems for critical applications will be designed, installed, operated and maintained to survive an intentional cyber assault with no loss of critical function.[27] This goal and the path to achieving it are presented in the January 2006 *Roadmap to Secure Energy Sector Control Systems for the Future*.

2. DHS and SSAs collaborate with owner/operator sector partners to develop sector-specific roadmaps, using the Energy Sector Roadmap as a model.

3. DHS promote uniform acceptance across all sectors that investment in control systems cyber security is a priority. For sectors with regulatory oversight of earnings and investments, DHS should promote inclusion of the costs of control systems cyber security as legitimate investments and expenses that deserve approval by their regulatory bodies.

4. DHS and other relevant Federal agencies implement recommendations for needed information sharing, outlined under the findings section for Improved Information Sharing.

5. DHS and other relevant Federal agencies implement recommendations for educating executive leaders of the cyber risk to critical infrastructure control systems, outlined in the findings section for Executive Leadership Awareness and in the framework in Appendix A.

B. *Market Drivers*

The NIAC found inconsistent market drivers across the sectors to develop and implement secure products and systems because the control systems market is in the early stages of a transition. Awareness of the security issues and needs is uneven across the critical infrastructure sectors, and the cost of developing and implementing security features is prohibitive for many operators and vendors.

Control systems are beginning a transition from proprietary, analog systems run over leased lines to a digital, IP-based architecture. This transition is in its early stages in the

[27] Roadmap to Secure Control Systems for the Energy Sector, January 2006, pp. 17.

market, and robust cyber security features are not currently available from many vendors and on many types of control systems.

Historically, control systems have operated in an isolated environment in which network security was unnecessary. As a result, there is no history of market demand for control systems security.

Today, these systems are converging, exposing control systems to IT-system attacks and vulnerabilities. Most control systems lack security features and practices common to IT systems. Some market drivers that exist in the IT market are not present in the control systems market. IT markets have a higher technology refresh rate, a consolidated vendor market, a large and diverse consumer market, relatively lower cost for systems, and demand for embedded security. In contrast, control systems can have a lifecycle of more than 30 years and represent enormous investments by their operators.[28] In some cases, operators leverage nearly the entire life cycle of a system to finance its purchase. Control systems operators are fewer than IT consumers and often run unique systems developed and implemented by small vendors.

One structural market barrier to achieving secure control systems is that there is no common set of security requirements or features for control systems between vendors and operators. In the existing market, improving control system security is difficult because operators cannot afford custom-built security solutions for each system and vendors cannot justify the cost to develop and build solutions without needed common security design goals.

The NIAC's research identified one effort that is beginning to address these existing market barriers to achieving control systems security – the *Cyber Security Procurement Language for Control Systems* project. A partnership among the New York State Office of Cyber Security and Critical Infrastructure Coordination, Idaho National Laboratory (INL), and the SANS Institute, the project relies on volunteer participation and feedback from control systems asset owners and vendors. This program is building a systematic approach for control systems operators to communicate their needs to control systems vendors. INL researchers are writing the document relying on cyber vulnerabilities identified in testing control systems with vendors and operators.

This market driver is building a usable method for procuring secure systems, complete with sample contract language, and is providing vendors with a common set of security features and a clearly identified market of interested buyers. If successful, this project will establish the common language for operators and vendors to communicate control systems security needs, providing a market-based solution.

Many operators are too small to demand security for their systems and cannot purchase the security features they need. Partners working on the *Cyber Security Procurement Language for Control Systems* are also using the process outlined in this document to

[28] From conversations with Study Group member and subject matter expert, Bill Muston, January 2006.

pool procurements for groups of smaller, revenue-restricted operators and help them acquire needed security.

The NIAC found that some sectors appear to have sufficient market drivers for developing needed security, while other sectors do not. The NIAC has developed a framework for guiding government regulators when considering market interventions. Each sector can apply this same framework for self-governance to establish needed conditions for appropriate market drivers. Further, if government is considering intervening in a sector's control systems market to improve cyber security, the NIAC Best Practices Framework should be applied to that process.

Recent trends in some sectors are showing implementation of control systems on current, standard operating systems – this provides both an opportunity and a danger for implementing improved cyber security.

Although long-term security implementations should include broad system replacement and upgrades, the private sector can accomplish much without costly wholesale system replacement. Existing IT security solutions (e.g., Common Criteria, NIST FIPS and Special Publications,[29] and sector-specific standards or solutions) can and should be implemented in the control systems environment. Products produced using these existing security and security-relevant standards and criteria can significantly improve the security posture of a system.

After careful consideration, the NIAC does not advocate mandating sector-specific standards across all sectors. This is consistent with the NIAC's previous approaches to effective infrastructure protection partnership.

Recommendations for Market Drivers

To achieve appropriate market drivers for secure control systems, the NIAC recommends:

1. OMB mandate that Federal agencies apply the *Procurement Language for Control Systems Security* document processes, as well as existing security and security-relevant standards and criteria when procuring control systems and services.

2. DHS and the SSAs encourage the application of existing security and security-relevant standards and criteria in the development and implementation of secure control systems.

[29] The Common Criteria is an international standard (ISO/IEC 15408) for computer security that does not specify a list of product security requirements or features. More information available at: http://www.commoncriteriaportal.org/. Federal Information Processing Standards (FIPS) are standards developed by the Federal government for use by all non-military government agencies and by government contractors. More information is available at: http://www.itl.nist.gov/fipspubs/.

3. DHS and the SSAs encourage owners and operators to identify and utilize existing security and security-relevant standards and criteria for their control systems. The process of applying these standards and criteria will provide the basis for continuing development of each operator's requirements to achieve control systems security.

4. SCCs apply the sector self-governance approach outlined in the framework of the NIAC's *Best Practices for Government to Enhance Security of the National Critical Infrastructures* April 2004, with validation by the SSA for evaluation of self-governance effectiveness within each sector and as an educational tool to establish reasonable sector steps to improve self-governance.[30]

C. *Executive Leadership Awareness*

The NIAC found that executive leadership awareness of the cyber threat to control systems, within government and industry operators and vendors, is critical to achieving needed action.

As the primary decision makers, executive leaders have the authority to make the needed changes. Moreover, private-sector executives make their company's strategic decisions, including risk assessments, and the government cannot prescribe specific actions to achieve needed security. The partnership between the private sector and government for critical infrastructure protection is relatively new and requires careful consideration of relationship management strategies. The NIAC found true executive awareness cannot be achieved by issuing government warnings. Instead, trust must be built through dialog, information sharing, and education. Continuing dialog and partnership is necessary to maintain an effective response to this dynamic threat.

Risk assessments are fundamental to strategic decisions by executives, but most executives lack a clear understanding of the cyber threat environment in which their control systems operate. Therefore, they do not fully understand the risk they are assuming. Safety is a core value for all critical infrastructure operators, and safety policy decisions require accurate risk assessments. The Federal government collects the threat information that executives need to make accurate risk assessments.

The non-profit research group, the U.S. Cyber Consequences Unit (US-CCU) has developed a model for initiating the conversation with executives about the emerging cyber threat. The US-CCU has found that executives will accept and make use of viable strategic information if it is presented to them. The first step involved is a dialog in which executive leaders begin thinking critically about the vulnerabilities that cyber threats create to their company's strategic position. This conversation must occur at a strategic level and it should include information on potential hostile actors, economic

[30] Available at: www.dhs.gov/niac/xlibrary/assets/niac/NIAC_BestPracticeSecurityInfrastructures_0404.pdf

motivators for hostile actors, operational and economic consequences, and existing cyber threats.[31]

The needed conversation with executive leaders will not take place unless the government can assure them that their shared information will be protected from public disclosure. The CIPAC framework and the SCCs offer an established, protected forum for this type of discussion.

The Protected Critical Infrastructure Information (PCII) program, established by the Critical Infrastructure Information Act of 2002, part of the law that created DHS,[32] has the potential to protect ongoing intra- and inter-sector communication in the future, but it has not yet resulted in adequate trust and understanding within the private sector. DHS is working to build the trust needed for PCII to fill this important role.

The NIAC found that communication of the cyber risk to critical infrastructure control systems is needed for all executive leaders, in both private- and public-sector organizations involved in infrastructure protection. Outreach efforts related to the *Cyber Security Procurement Language for Control Systems* identified government executives in all levels of government as a critical group needing education and awareness.[33]

Recommendations for Executive Leadership Awareness

To improve executive leadership awareness of the cyber risk to control systems, the NIAC recommends that:

DHS work with SSAs to implement a program for control systems cyber security executive awareness outreach. This outreach will include the elements outlined in the attached Framework in Appendix A. Key elements of the outreach program include:

- Value for senior executive-level decision-maker participants through inclusion of relevant strategic threat information gathered by the Intelligence Community.
- Establishment of a continuing dialog among all parties relevant to critical infrastructure control systems in the public- and private-sectors, owner-operators and supporting government agencies, and vendors involved in control system implementations, including IT and Security.
- A protected forum for discussion of strategic information through use of the Critical Infrastructure Partnership Advisory Council (CIPAC) framework and SCCs.
- Awareness outreach to address executive-level decision makers in critical infrastructure owner-operators and relevant decision makers in SSAs, State, and local government.

[31] Study Group discussions with Scott Borg of the US-CCU.
[32] Critical Infrastructure Information Act of 2002, paragraphs 211-214 of the Homeland Security Act of 2002, Public Law 107-296
[33] From Study Group discussion with Director of New York State Office of Cyber Security and Critical Infrastructure Coordination, Will Pelgrin, August 31, 2006.

- Strategic-level conversations to achieve operator vulnerability self-discovery, making use of strategic-level information on threats, hostile actors, economic motivators for hostile actors, and economic and physical consequences.
- DHS promotion of critical infrastructure control systems vulnerability assessments for development of corporate awareness.
- Education of executives that control systems cyber security is critical to the corporate goal of operational safety.

D. *Government Leadership Priorities*

The NIAC found strong and committed government efforts underway (see Appendix D) to address the cyber threat to control systems. Government actions could benefit from private sector feedback, and higher-level interagency coordination and strategic planning to address the cyber threat to control systems.

Notable existing Federal efforts to address this threat include DHS' Control Systems Security Program (CSSP), under the National Cyber Security Division (NCSD), the U.S. Computer Emergency Readiness Team (US-CERT), and DHS' Science and Technology (S&T) Directorate. Additionally, the Department of Energy's *Roadmap to Secure Control Systems for the Energy Sector* and research efforts such as the National SCADA Test Bed (NSTB) at the National Laboratories (see Appendix D) are underway to study the threat. These programs show the dedication, commitment, and appropriate concern within the Federal government for protection of these important assets. Further, the NIAC found these existing programs are communicating with each other and looking to leverage each other's work where possible to provide private and public sector critical infrastructure operators the knowledge and resources they need.

However, the NIAC also found that the roles and responsibilities of various stakeholders are not always clear. Although DHS has the authority to lead this critical infrastructure protection effort, there are other authorities in different sectors that have the potential to create conflicting directions. Also, communication and cooperation among Federal agencies often appears to be on an ad hoc basis. High-level accountability and participation would strengthen coordination, developing a strategic planning commitment to the Federal government's response to the cyber threat to critical infrastructure control systems.

To coordinate and prioritize Federal cyber security Research and Development (R&D) expenditures, the Office of Science and Technology Policy (OSTP) and OMB establish high-level research priorities. OSTP, through the National Science and Technology Council (NSTC), and its interagency working group, the Cyber Security and Information Assurance Interagency Working Group (CSIA-IWG), produces the *Federal Plan for Cyber Security and Information Assurance Research and Development*, which prioritizes and coordinates existing Federal cyber security R&D programs. OSTP uses this report to establish appropriate funding in the budget that the President submits to Congress each year. The recent establishment of this process is a significant achievement. However, the

NIAC found this process could benefit from private-sector input on needed technology to better adapt to the emerging threat.

Another opportunity for Federal government leadership uncovered by the NIAC is the opportunity to utilize available government resources to communicate the control systems cyber security message to the private sector. NIAC learned that many companies and governing boards use the Malcolm Baldridge Award for Excellence in Business Management to establish internal standards and metrics.[34] This award, presented annually by the U.S. Department of Commerce, presents an opportunity to raise awareness of this important issue.

Recommendations for Government Leadership Priorities

To improve Federal government leadership in the effort to address the cyber risk to control systems, the NIAC recommends:

1. SSAs assign a senior executive leader, at a level equivalent to or higher than the DHS Assistant Secretary for Cyber Security and Communications, responsible and accountable for their agency's collaboration with DHS efforts to address control systems cyber security for their sector. This group will be responsible to meet annually with the PCIS to evaluate each sector's strategy to meet the national goal set for 2015.

2. The Federal government incorporate private sector input into the cyber R&D funding prioritization processes conducted by OSTP and OMB. To begin, this process should consult relevant SSPs as a means of gathering input. SSAs will be responsible for establishing additional avenues for gathering and incorporating this important information.

3. As a collaborative effort to increase executive awareness, the NIAC recommends DHS work with the Malcolm Baldridge Award for Excellence in Business Management and other similar programs to help communicate the importance of control systems cyber security to business leaders.

E. *Information Sharing*

The NIAC found that improved sharing of information on control systems threats, vulnerabilities, incidents, and solutions is vital to a properly informed and measured response to the threat to critical infrastructure control systems.

During its investigations, the supporting Study Group identified a need for trusted and protected information sharing mechanisms for tactical, operational, and strategic-level information about control systems cyber risk. Some mechanisms exist and are being used for sharing vulnerability information as control systems vulnerabilities appear. Additionally, US-CERT and its supporting organizations are beginning to develop processes required to mitigate control systems vulnerabilities.

[34] Website: www.quality.nist.gov

Models exist that validate the value and viability of incident information sharing. The Industrial Security Incident Database (ISID), compiled by Dr. Eric Byres (formerly part of the British Columbia Institute of Technology (BCIT) and Wurld Tech Inc.) in Vancouver, British Columbia, collects and aggregates cyber incident information to share with database contributors.[35] The NIAC found that this is the only widely known database available to control systems operators, and its sample of incidents is limited in size and accessibility. This kind of information is needed to increase awareness and understanding of the threat among control systems operators, and to better inform important cyber risk assessments for critical infrastructure control systems.

A complicating factor to achieving effective incident information sharing is that private-sector operators are very resistant to sharing information about cyber attacks on their control systems. Operators believe that cyber incidents affecting operations, if known publicly, could expose their company to further attacks. Such exposure could also undermine shareholder confidence, which could adversely affect stock prices. An established, trusted, and protected mechanism is required to successfully collect and share cyber incident information with control systems operators. Because some operators are reluctant to share this information with the government, this mechanism must be established outside the government.

To interact effectively with the control systems operator community to collect and aggregate cyber incident data, the collecting organization will need to build trusted relationships by providing value-added services to operators. Over the past 18 years, CERT/CC has developed the resources and processes to make it capable of serving in this role while establishing itself as a widely recognized multi-vendor, international coordinator for the IT sector. With similar programs and services, this model could be applied to the control systems community. CERT/CC's long history and experience in supporting the IT sector gives it background, understanding, and institutional processes that could serve as a model for a trusted, third-party coordinator. US-CERT has recently initiated activity in this area at CERT/CC.

The Department of Energy's National Laboratories are involved in important work with vendors and operators on control system vulnerabilities, research, configuration testing, and development of best practices. However, a cross-sector third-party coordinator, like CERT/CC, is required to manage control system vulnerability and incident information.

Strategic threat information is important to understanding the cyber risk to control systems and key to establishing a dialog and raising awareness among critical infrastructure executive leaders. The NIAC looked into what threat information was available from the Intelligence Community for this purpose. Discussions uncovered that the Intelligence Community is broadly reluctant to share the information it has collected on cyber threats outside the Intelligence Community. Even though intelligence agencies may be aware of the cyber threat to critical infrastructure control systems, there is no

[35] Discussion with Dr. Eric Byres, BCIT, March 9, 2006.

established existing mechanism to share this information with critical infrastructure operators.

DHS has responsibility for communicating strategic threat information to private sector infrastructure operators, and DHS' Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) organization is responsible for developing these threat products. But because HITRAC does not own much of the information, their efforts to share with the private sector are hampered by the Originator Control (ORCON) legal limitations and procedural requirements. ORCON rules require HITRAC to follow varying and agency-specific procedures before they are allowed to share information with their private sector constituency.[36] The result appears to be that the government is communicating very little useful information to the private sector. The NIAC supports the findings of the *NIAC Public-Private Sector Intelligence Coordination Final Report*, which called for standardized marking and restrictions to improve information sharing.[37]

Adequate control systems cyber protection also demands that critical infrastructure protection partners be proactive and use all available information and expertise to anticipate future problems, trends, and needs. DHS and critical infrastructure partners share a common mission and must collaborate to apply available expertise to known information to achieve understanding of the cyber threat. This function could allow DHS and critical infrastructure operators to maintain a broad view of the cyber risk, making it possible to anticipate emerging issues and threats and then issue specific, targeted warnings to affected sectors.

The NIAC found that the Information Sharing Environment, created to integrate terrorist information across all Federal agencies,[38] could be a critical communication node for cyber threat information. Use of a robust, protected information sharing mechanism such as this would increase the visibility and usefulness of relevant control systems cyber threat information.

Recommendations for Information Sharing

To improve information sharing about control systems threats, vulnerabilities, and risks, the NIAC recommends:

1. DHS enhance the control system cyber incident information collection mechanism at CERT/CC for comprehensive collection, protection and sharing.

2. DHS rapidly ramp up CERT/CC's support services for control system operators to help develop a capability to collect cyber incident information.

---

[36] Study Group discussions with DHS HITRAC, November 9, 2006.
[37] http://www.dhs.gov/xlibrary/assets/niac/niac_icwgreport_july06.pdf (page 28).
[38] The ISE was formally created by the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 to facilitate terrorism information sharing in accordance with Executive Orders 13311 (July 11, 2003) and 13388 (October 25, 2005) and the Homeland Security Act of 2002.

3. DNI develop a solution to the problem of originator control (ORCON) that prevents DHS from sharing threat information with critical infrastructure operators.

4. The Intelligence Community produce a Threat Assessment for control systems to begin the process of establishing a knowledge base about this emerging and dynamic threat. Also, the Intelligence Community produce a National Intelligence Estimate (NIE) on the cyber threat to critical infrastructure control systems.

5. DHS share relevant information from the Threat Assessment and NIE with critical infrastructure control systems operators to help them understand the threat.

6. DHS enhance existing program activities to create the ability to integrate and track understanding of the cyber risk for critical infrastructure control systems using all available sources.
   - This collaborative program should collect, correlate, integrate, and track information on:
     - threats, including adversaries, toolsets, motivations, methods/ mechanisms, incidents/actions, and resources;
     - consequences, including potential consequences of compromise to sector, industry, and facility-specific control systems; and
     - vulnerabilities in control systems or their implementations in the IT infrastructure that adversaries could exploit to gain access to critical infrastructure control systems.
   - This capability is a DHS operations function, and will include input and expertise from: critical infrastructure owner/operators and other relevant parties in the private sector regarding consequences and vulnerabilities, the Intelligence Community regarding threats, CERT/CC and other sources regarding incidents, and DHS (including US-CERT) regarding cyber vulnerabilities.
   - DHS will communicate resulting warning information to control systems owner-operators to ensure protection of U.S. critical infrastructures.

7. The Program Manager, Information Sharing Environment, include information on control systems cyber threats in the President-directed and Congress-mandated Information Sharing Environment (ISE).

VI. CONCLUSION

The Council found the threat to critical infrastructure control systems from the convergence of physical and IT systems is very real and growing rapidly.

Critical infrastructure operators with control systems face a new and increasing threat due to the convergence of their physical control and IT systems. Critical infrastructure control systems are no longer isolated, and as a result, face exposure to Internet IT vulnerabilities. The diversity of these systems, the differences among the sectors, the challenges presented with the convergence of these two types of systems, and the dynamic nature of the threat present significant challenges to developing a solution to this problem. Other obstacles include lack of awareness and understanding of the risk posed by convergence and cyber threats.

Clearly, there are important roles for government to support the public-private partnership for protecting critical infrastructures. The government should continue to look for their appropriate role in this relationship by identifying best practices, nurturing the marketplace to adapt to the emerging challenges, and by working to build relationships with the private sector to solidify the partnership for critical infrastructure protection. Government should also provide resources within a careful, methodical, disciplined framework, where the market does not move quickly enough to meet national security requirements, and play a critical role in educating stakeholders about the emerging threat.

The NIAC found identifiable policy changes that can help to address this risk. Improved executive awareness of the problem, combined with needed information sharing about threats, incidents, and vulnerabilities, and a measured and coordinated Federal government response and implementation can help move us toward the goals for securing our Nation's critical infrastructure control systems.

APPENDIX A: FRAMEWORK FOR EXECUTIVE OUTREACH

The following is framework guidance for the critical infrastructure control systems cyber security outreach program:

1. Outreach should seek to communicate an understanding of system vulnerabilities and the cyber threat to control systems to elected and appointed senior leadership executive decision-makers. Moreover, the outreach effort should highlight the importance of these systems, the risks involved, and the negative impact of their loss.
2. The primary entities for communication are control system owners and operators in the public and private sectors, control systems vendors and solutions providers, the relevant Federal, State, and local regulatory bodies, and infrastructure protection partners in the Federal, State, and local governments.
3. A secondary audience of insurance and bonds rating executives should also be considered.

Systems owners and operators
Outreach should communicate with elected and appointed senior executive leaders to reach an audience that can implement the actions necessary to correct vulnerabilities and address the threat.

Control system vendors and solution providers
Outreach should encourage development of inherently secure systems and solutions as well as necessary security upgrades for existing legacy systems, given the current state of converged systems and the growing threat.

Relevant Federal, State, and local regulatory bodies
Outreach should educate regulatory bodies on the nature of the threat, the importance of these systems, and the growing risk to our infrastructure, in an effort to ensure regulators understand the need for increased security investment by owner-operators.

Infrastructure partners in the relevant Federal, State, and local agencies
Outreach should stimulate awareness of the importance of control systems, the impact of their loss, and the threats and vulnerabilities to control systems in order to generate the necessary understanding and support for operator solutions in their respective sector, State, or locality.

Regardless of audience, there are four critical content elements:

1. Specific and current threat information
2. General and specific vulnerability information
3. Economic and physical consequences of cyber attacks
4. What can be done to improve cyber security of control systems

Threat information needs to be credible information developed by all available sources within the Intelligence Community. The information should contain all potential hostile actors and be shared at the highest possible classification level to best illustrate the nature of the problem for the intended audience.

General and specific vulnerability information should contain both high-level and specific information on how vulnerabilities can compromise a company's operations and create liabilities. Initial conversations should cover the dynamics of the involved issues and communicate the importance and rapid acceleration of activity in control systems attacks. Conversation should share available compiled incident data and wherever possible, real vulnerability-incident-consequence scenarios to improve understanding and appreciation of the problem.

Economic consequences of cyber attacks should present a commonsense economic analysis of the cyber threat to control systems in easily accessible, strategic-level terms that will speak directly to executive decision makers and facilitate a process of strategic vulnerability self-discovery, independent of intelligence threat assessments. The U.S.-Cyber Consequences Unit (US-CCU) has developed and presented a good example of the material and process needed here, covering economic consequences of cyber attacks, the spectrum of potential hostile actors, and economic motivators for hostile actors.

To address the problem, participants should gain an understanding of what policy, procedural, technical, and training/awareness initiatives exist. Executive participants in the discussion should also gain a number of insights through this process, including:

- an understanding of the available resources, the required budget, issues involved, and be able to set priorities and goals as a result;
- an appreciation for the value of vulnerability assessments in gaining understanding of their current security posture and in establishing a culture of security in the control systems environment; and
- an understanding and appreciation for the value of improved cyber incident information sharing and how they can safely participate in this exchange.

Executive awareness outreach by the Federal government will be organized under the leadership of DHS, involve each sector's SSA, and use established, trusted, and protected mechanisms for communication of this sensitive information to the private-sector owners and operators. To achieve this, the CIPAC framework, including the SCCs and GCCs should be used as the communication mechanism in these outreach efforts.

DHS' executive awareness outreach should seek to establish a collaborative and ongoing conversation. Presentations to executives should undergo a vetting process with set standards regarding content, for usefulness, relevance, and timeliness to preserve the trust of participating executives.

Organizers should ensure that they base these outreach programs in facts and validated analysis, and should include recent changes and trends. Presentations should be sensitive

to and incorporate audience concerns, leveraging participants' own knowledge of their businesses with a self-discovery process through conversation. Cross-sector collaboration in these conversations should be particularly sensitive to differences among the sectors.

APPENDIX B: NATIONAL INFRASTRUCTURE ADVISORY COUNCIL MEMBERS

NIAC CHAIR
Mr. Erle A. Nye, Chairman Emeritus, TXU Corp.

MEMBERS
Mr. Edmund G. Archuleta, General Manager, El Paso Water Utilities
Dr. Craig R. Barrett, Chairman of the Board, Intel Corporation
Mr. Alfred R. Berkeley, III, Chairman & CEO, Pipeline Financial Group LLC, *(Vice Chairman (ret.) NASDAQ)*
Mr. George H. Conrades, Executive Chairman, Akamai Technologies
Chief Rebecca F. Denlinger, Chief, Cobb County (Georgia), Fire & Emergency Services
Lt. Gen. Albert J. Edmonds (ret.), Chairman, Edmonds Enterprise Services, Inc
Chief Gilbert L. Gallegos (ret.), Chief of Police, City of Albuquerque, New Mexico
Ms. Margaret E. Grayson, President, Grayson and Associates
Commissioner Raymond W. Kelly, Police Commissioner, New York Police Department
Ms. Martha H. Marsh, President & CEO, Stanford Hospital and Clinics
Mr. James B. Nicholson, President and CEO, PVS Chemical, Inc.
Mr. Thomas E. Noonan, General Manager, IBM, Internet Security Systems
Hon. Tim Pawlenty, Governor, State of Minnesota
Mr. Gregory A. Peters, Managing Partner, Collective IQ
Mr. Bruce Rohde, Chairman & CEO Emeritus, ConAgra Foods
Dr. Linwood H. Rose, President, James Madison University
Mr. John W. Thompson, Chairman & CEO, Symantec Corporation

APPENDIX C: RESOURCES

Additional Study Group Resources: Subject Matter Experts

Mr. George Beitel, Idaho National Laboratory
Mr. Scott Borg, U.S. Cyber Consequences Unit
Dr. Eric Byres, British Columbia Institute of Technology
Dr. George Cybenko and Dr. Sean Smith, Dartmouth College
Mr. Thomas Flowers, CenterPoint Energy, NERC
Mr. Tom Hanigan, DuPont Corporation, Pioneer Agriculture Seed Division
Mr. Stan Johnson, North American Electric Reliability Council
Mr. Henry Kenchington, Department of Energy
Mr. Miles Keogh, National Association of Regulatory Utility Commissioners (NARUC)
Dr. Thomas Longstaff, Carnegie Mellon Software Engineering Institute (CERT/CC)
Mr. Doug Maughan, DHS Directorate for Science and Technology
Mr. Reggie McKinney, DHS US-CERT
Mr. Bob Mick, ARC Advisory Group
Mr. William Pelgrin, New York State Infrastructure Coordination Office
Mr. Jeff Pillon, NARUC
Mr. Venkat Pothamsetty, Cisco Systems Corporation
Mr. Francisco Ramirez , DHS US-CERT
Mr. Julio Rodriguez, Idaho National Labs/DHS NCSD Control Systems Security Program
Mr. Paul Skare, Siemens Corporation
Mr. Michael Torppey, Process Control Systems Forum
Ms. Rita Wells, Idaho National Labs
Mr. Michael Witt, DH US-CERT
Mr. Andrew Wright and, Cisco Systems Corporation

BIBLIOGRAPHY

Executive Office of the President of the United States of America. (February 2003). *The National Strategy to Secure Cyberspace*. DC: U.S. Government Printing Office.

Borg, S. and Bumgarner, J. (2006). *The US-CCU Cyber Security Checklist. VT:* U.S.-Cyber Consequences Unit.

Borg, S. "Notes for the NIAC Cyber Convergence Working Group" (brief), US Cyber Consequences Unit, April 2006.

Byres, Eric. "New and original study on industrial cyber security reveals tenfold increase in number of successful attacks on process control and SCADA systems since 2000," (October 04, 2004). BC: British Columbia Institute of Technology.

Energetics Inc. (January 2006). *Roadmap to Secure Control Systems in the Energy Sector*, DC: U.S. Department of Energy and U.S. Department of Homeland Security.

Department of Homeland Security. (2006). *National Infrastructure Protection Plan.* DC: U.S. Government Printing Office.

Department of Homeland Security National Cyber Security Division, (September 2006). *Cyber Storm Exercise Report*. DC: U.S. Department of Homeland Security.

Government Accountability Office. (March 2004). *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*. DC: U.S. Government Printing Office.

Government Accountability Office. (September 2006). *Information Security: Coordination of Federal Cyber Security Research and Development.* DC: U.S. Government Printing Office.

Idaho National Laboratory - Control Systems Security and Test Center. (September 2004). *Evaluation of Control Systems Security Related Programs*. DC: U.S. Department of Homeland Security

Idaho National Laboratory - Control Systems Security and Test Center. (August 2005). *Cyber Incident Report for US-CERT Control Systems Security Center (Status Report)*. DC: U.S. Department of Homeland Security

Idaho National Laboratory, Battelle Energy Alliance. (August 2006) *Cyber Security Procurement Language for Control Systems (Draft 1.4)*, DC: Department of Homeland Security.

Lawton, R., Wilhelm, J.D., Burns, R.E., Potter, S., McGarvey, J. (July 2004). *Model State Protocols for Critical Infrastructure Protection Cost Recovery,* DC: National Association of Regulatory Utility Commissioners.

Mick, R. (January 2006) *ARC Advisory Group Manufacturing Security Brief to NIAC Study Group*.

National Science and Technology Council Interagency Working Group on Cyber Security and Information Assurance. (April 2006). *Federal Plan for Cyber Security and Information Assurance Research and Development.* DC: U.S. Government Printing Office.

National Infrastructure Advisory Council. (October 2004). *Common Vulnerability Scoring System Final Report and Recommendations by the NIAC*. DC: U.S. Department of Homeland Security.

National Infrastructure Advisory Council. (October 2004). *Prioritizing Cyber Vulnerabilities Final Report and Recommendations by the Council.* DC: U.S. Department of Homeland Security.

National Infrastructure Advisory Council. (April 2006). *Workforce Preparation, Education and Research Working Group Final Report and Recommendations by the Council.* DC: U.S. Department of Homeland Security.

National Infrastructure Advisory Council. (July 2006). *Public-Private Sector Intelligence Coordination Final Report* DC: U.S. Department of Homeland Security.

Shea, D., Congressional Research Service - Library of Congress. (July 2003). *Critical Infrastructure: Control Systems and the Terrorist Threat.* DC: U.S. Government Printing Office.

APPENDIX D: THE CURRENT STATE OF SECTOR AND FEDERAL EFFORTS TO ADDRESS CONTROL SYSTEMS SECURITY

During its research, the supporting NIAC found a dedicated community of individuals and programs committed to addressing the emerging cyber threat to critical infrastructure control systems. This community spans from the Federal government to the private sector, and from academia to State and local governments. The most successful and promising programs were collaborative efforts with effective communication and planning. Following is a brief list of the most significant and effective efforts that the supporting Study Group discovered.

Ongoing Federal Government Programs and Efforts

The most significant federal efforts to improve the cyber security of critical infrastructure control systems originate from DHS and the Department of Energy (DOE). The National Cyber Security Division (NCSD), under the Cyber Security and Communications (CS&C) directorate at DHS, has been assigned the authorities to address the cyber threat to the U.S. critical infrastructure control systems, as is outlined in the *National Plan to Secure Cyberspace* and HSPD-7. NCSD has established the Control Systems Security Program (CSSP) within its Strategic Initiatives branch to carry out this work. CSSP is the only organization in the Federal government that has a mission specific to addressing cyber security for control systems.

Currently, CSSP's is focused on high-return collaborative efforts to improve awareness and resources for control systems operators seeking to improve the cyber security of existing (legacy) and emerging (next generation) control systems. CSSP coordinates between other Federal government efforts, seeking to leverage existing work. CSSP also sponsors important work, such as the Control Systems Security Center (CSSC) at the Idaho National Laboratory (INL), where, in collaboration with vendors and operators, INL tests control systems for vulnerabilities and potential security solutions. The very promising *Cyber Security Procurement Language for Control Systems* document is another program sponsored by CSSP at the INL CSSC. Other significant efforts by the CSSP include development of a Control Systems Cyber Security Self Assessment Tool (CS^2SAT).

CSSP sponsors and collaborates with standards bodies, such as National Institute of Standards and Technology (NIST) and the Instrument Society of America (ISA), on development of cyber security standards. CSSP is involved in sector-specific efforts, including the Critical Infrastructure Protection (CIP) standards currently under review by the North American Electric Reliability Council (NERC). CSSP is working to cross reference standards, recommended practices, and other control systems security tools including the CSSP CS^2SAT and the *Cyber Security Procurement Language for Control Systems* document to assist operators in finding solutions to identified vulnerabilities.

In support of the U.S. Computer Emergency Readiness Team (US-CERT) mission, CSSP augments existing capabilities for control systems incident reporting and vulnerability

issues. US-CERT is a division of DHS' NCSD and is responsible for responding to cyber incidents and coordinating vulnerability mitigations and solutions for cyber issues within the Federal government. While officials at US-CERT spend most of their time addressing IT cyber vulnerabilities and incidents, they are very aware of the cyber risk to critical infrastructure control systems and have resources specifically designated to address this threat. US-CERT also has a 24/7 operations center that works constantly to identify, track, and mitigate cyber vulnerabilities, including those for control systems. In this effort, US-CERT sponsors and works in close coordination with Carnegie Mellon's Computer Emergency Response Team Coordination Center (CERT/CC) maximizing the resources and knowledge of both organizations to address this problem.

DHS' Science and Technology Directorate (S&T) is involved in cyber security Research, Development Testing and Evaluation (RDT&E) efforts, some of which include control systems. S&T's efforts provide funding for efforts in collaboration with private sector operators and DOE efforts.

Each of the critical infrastructure sectors operating control systems is engaged to differing degrees with the SSA to address the cyber threat to control systems. The Energy sector is leading the critical infrastructure sectors in developing and implementing cyber security solutions for control systems. DOE's leadership and program is a critical component of that success. The DOE Office of Electricity Delivery & Energy Reliability (OE) leads this effort and is coordinating with DHS. OE is a significant source of funding for control systems security solutions in the Energy sector, most of this work being carried out through the National SCADA Test Bed (NSTB) program, sponsored by DOE and carried out at INL and Sandia National Laboratories (SNL). The NSTB program works with vendors and operators to test next generation control system configurations for vulnerability to cyber attacks, and it also tests and evaluates potential solutions to identified vulnerabilities.

OE sponsored the development of *The Roadmap to Secure Energy Sector Control Systems for the Future*, a carefully constructed strategic plan for significantly increasing the resilience of Energy sector control systems to cyber attacks by the year 2015. This document, although specific to the Energy sector, could also be used as a model for strategic planning with other critical infrastructure sectors. Currently, the Department of Energy is using the roadmap to plan RDT&E funding and program development within the Energy sector. DHS' CSSP coordinates with OE and the NSTB to leverage the Energy sector's accomplishments across all CI/KR sector program efforts and avoid duplication of effort.

Another significant Federal program is the CSSP-sponsored Process Control Systems Forum (PCSF). PCSF is a collaborative organization of professionals in the private sector and government committed to developing solutions to the cyber threat to control systems. PCSF meets annually and is a forum for collaboration between the public and private sectors, including owner-operators and vendors (both IT and control systems), to address this emerging set of threats and vulnerabilities. PCSF also assembles working groups to generate solutions and develop stakeholder participation.

As noted in the discussions above regarding the work of both DOE and DHS, the National Laboratories are providing critical technical contributions to the effort to secure control systems from cyber threats. Different agencies each sponsor different laboratories to provide technical support to their programs, conducting the research, development, and testing for the solutions and recommended practices needed to improve today's cyber security of critical infrastructure control systems. CSSP conducts its work at INL's CSSC and includes several of the national laboratories. Researchers at Sandia National Laboratory support DHS S&T's RDT&E efforts. DOE's NSTB effort is co-lead with INL and SNL. Other officials are carrying out other control systems cyber security work at Pacific Northwest National Laboratories, Lawrence Livermore National Laboratory, Argonne National Laboratory, and Oakridge National Laboratory. The national laboratories compete to support these federal programs, but work together closely to support this important effort.

The National Institute of Standards and Technology (NIST), under CSSP sponsorship, is actively involved in developing standards for use in control systems security. NIST is currently reviewing the recently developed cyber security standards for control systems titled, *Guide to SCADA and Industrial Control System Security (NIST SP 800-82)*. Expected to be completed in early 2007, this document will provide broad guidance in establishing security for SCADA and process control systems and devices.

There are other Federal government programs working to develop control systems cyber security solutions, but for a variety of reasons have chosen a lower visibility profile. One such effort is that of the Nuclear Regulatory Commission (NRC), which works with the Nuclear sector to secure those systems, but does not communicate with other Federal control systems cyber security programs.

OSTP and OMB direct the recently developed Federal government coordination for cyber security R&D efforts. OSTP coordinates development of a Federal research agenda for cyber security and oversees the National Science and Technology Council (NSTC), which prepares R&D strategies, coordinated across involved Federal agencies.[39]

The NSTC operates through its committees, subcommittees, and interagency working groups to strategically plan for cross-agency cyber R&D funding expenditures. The Subcommittee on Networking and Information Technology Research and Development (NITRD) and the Cyber Security and Information Assurance Interagency Working Group (CSIA-IWG) are prominently involved in identifying existing programs and shortfalls for coordination of cyber security research. The CSIA-IWG's *Federal Plan for Cyber Security and Information Assurance Research and Development* used in this process specifically addresses allocations for control systems cyber R&D.[40]

---

[39] *GAO Report: Prioritizing Cyber Security Research and Development in Government Funding*, September 2006, pp.12.

[40] From conversations with CSIA-IWG co-chair Annabelle Lee and also the *GAO Report: Prioritizing Cyber Security Research and Development in Government Funding*, September 2006.

Non-Federal and Collaborative Efforts

One promising effort identified during the Group's research was the collaborative *Cyber Security Procurement Language for Control Systems* document that is sponsored by CSSP and is currently under development at the INL. The project is also receiving major contributions in leadership from Mr. Will Pelgrin at the State of New York Office of Cyber Security and Critical Infrastructure Coordination. This office works with the SANS Security Institute to collaborate with vendors and operators, gaining feedback and stakeholder buy-in on the developed document. This process is closing a gap between operators who often do not know how to ask for needed security and vendors who are too often reluctant to develop solutions because operators each ask for specific and unique security implementations. The result is a usable set of procurement language for control systems cyber security measures that can be implemented at any point during the control systems procurement cycle. Not only does it provide operators with the means to contract for the security their systems need (which is a significant technical barrier for many operators) but it also is providing vendors with a common set of requirements they can build toward to meet the requirements of a broad set of customers. Document development is moving quickly, with the first iteration, covering basic control systems security implementations, being published in the first six months of work. Vulnerabilities and solutions identified in the document are real-world vulnerabilities and solutions that the CSSP and INL uncovered during their work with vendors and operators. This project has the potential to generate significant movement in the control systems security solutions market.

The CERT Coordination Center (CERT/CC) at Carnegie Mellon's Software Engineering Institute (SEI) is a Federally Funded Research and Development Center (FFRDC) involved in supporting US-CERT's work at DHS. Since its creation in 1988 by the Defense Advanced Research Projects Agency (DARPA) in the wake of the Morris computer worm, CERT/CC has been critical in developing coordinated responses to Internet cyber security incidents and managing IT vulnerabilities. CERT/CC has IT institutional knowledge, expertise and relationships to make a significant contribution to securing critical infrastructure control systems. CERT/CC is currently developing resources to address the emerging cyber risk to control systems.

The U.S. Cyber Consequences Unit (US-CCU) is a not-for-profit, independent research institute, founded by economist Scott Borg. Although the U.S. government funded US-CCU, it operates completely independent of the Federal government. The US-CCU's organizational independence and its practices for protecting the sensitive information of cooperating private-sector operators has provided access to information not available to other organizations, and with that, a unique perspective into the potential economic consequences of cyber attacks on private sector operators. Some products of the US-CCU's research are more sensitive and only shared with narrow, target audiences, but the more general and broadly applicable products, like *The US-CCU Cyber Security Checklist* are distributed to U.S. critical infrastructure operators and also internationally. The *US-CCU Cyber-Security Check List*, which was released in its final version in November 2006, is being currently being translated into eleven languages. US-CCU

founder Scott Borg participated in the Physical/Cyber Convergence Study Group as a subject matter expert and contributed to this report.

Some sectors and industries have moved to develop voluntary standards and practices to address the cyber security of their SCADA and control systems. Sector-specific standards nearing completion now include NERC's Critical Infrastructure Protection (CIP) standards 001 through 009. The CIP standards are currently under review by the Federal Energy Regulatory Commission (FERC) for potential use as the new regulatory standard for the electric sector, imposed by the Energy Reliability Act of 2005. These CIP standards provide a viable model for sector collaboration in development of voluntary control system cyber security requirements.[41] Similar efforts are underway in various sectors, including the Chemical sector.

Another noteworthy effort is the Industrial Security Incident Database (ISID), established in the late 1990s by Dr. Eric Byres at the British Columbia Institute of Technology (BCIT). The database includes over 200 cyber incident accounts submitted by control systems operators interested in learning more from the database, and the number continues to grow. Most significantly, the information contained in the database has been responsible for inspiring participants, particularly in the Energy sector, to invest significantly in improvements to their control systems' security posture.

Although there are many other current efforts to address the cyber threat to control systems, those listed above are the most significant and visible efforts identified by the NIAC during its research.

[41] Study Group conversation with Stan Johnson, NERC, August 10, 2006.