

# National Infrastructure Advisory Council (NIAC)

## Convergence Working Group

Final Report and Recommendations  
January 16, 2007

George H. Conrades  
Executive Chairman  
Akamai Technologies

Greg Peters  
Managing Partner  
Collective IQ

Margaret Grayson  
President, Grayson  
and Associates

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

## Overview

---

- Purpose
- Actions
- Timeline
- Potential NIAC Recommendations
- Next Steps

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

## Purpose

---

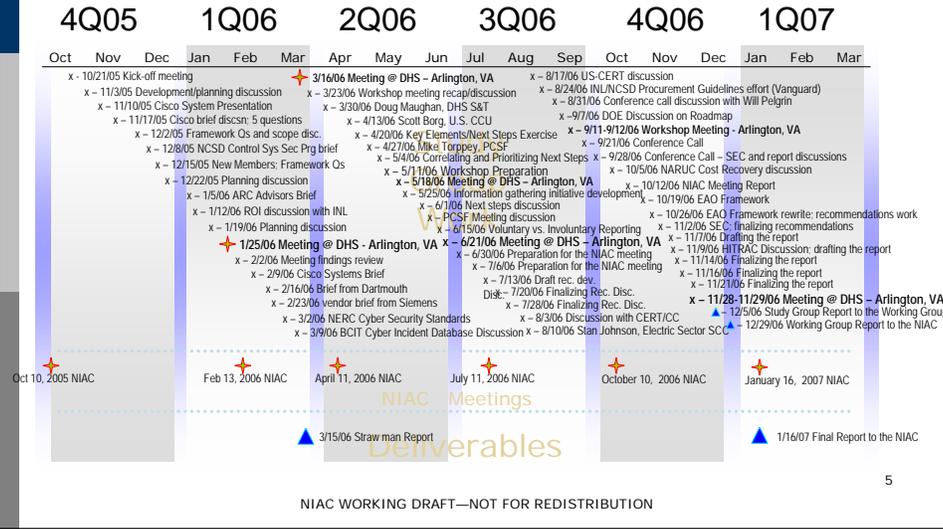
- **Mission:** The Convergence Working Group investigated important questions and to make recommendations regarding the protection of SCADA and Process Control Systems from cyber threats.

## Actions

---

- The Study Group doubled the pace of work in October and November - held 9 more (total of 52) conference call discussions to validate the recommendations and shape the Study Group Report.
- The Study Group held a 4-day workshop meeting at the end of November to rework the final Study Group Report to the Working Group.
- The Study Group Report was sent to the Working Group and selected subject matter experts on December 5, 2006.
- The Working Group Pre-briefed the White House regarding the potential recommendations on December 13, 2006.
- After feedback and revision, (including 4 more Working Group conference call meetings) the final Working Group Report was sent to the NIAC on December 29, 2006.

# Time Line



# Process: The Five Framework Questions

- ❑ **Security as an Enabler** - How do we 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?
- ❑ **Market Drivers** - What are the market drivers required to gain industry attention and commitment to research and product development?
- ❑ **Executive Leadership Awareness** - How do we 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?
- ❑ **Federal Government Leadership Priorities** - What are the appropriate Federal Government leadership roles and priorities in identifying threats, vulnerabilities, risks and solutions?
- ❑ **Improving Information Sharing** - What are the obstacles and recommendations for improving information sharing about Process Control Systems and SCADA threats, vulnerabilities, risks and solutions?

## Recommendations for Security as an Enabler

The Working Group 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.

### Recommendations:

- 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.
- The Department of Homeland Security (DHS) and Sector-Specific Agencies (SSAs) collaborate with their respective owner/operator sector partners to develop sector-specific roadmaps using the Energy Sector Roadmap as a model.
- 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.
- DHS and other relevant Federal agencies implement Convergence Study recommendations for Improved Information Sharing.
- DHS and other relevant Federal agencies implement Convergence Study recommendations for Executive Leadership Awareness and the framework in Appendix A.

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

## Recommendations for Improving Market Drivers

The Working Group 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 most operators and vendors.

### Recommendations:

- The Office of Management and Budget (OMB) mandate that Federal agencies apply the *Cyber Security Procurement Language for Control Systems* document and existing security and security-relevant standards and criteria when procuring control systems and services.
- DHS and the SSAs encourage the application of existing security and security-relevant standards and criteria in developing and implementing secure control systems.
- 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.
- 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. <sup>8</sup>

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

## Recommendations for Executive Leadership Awareness

The Working Group 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.

### Recommendations:

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 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 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.
- 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.
- Education of executives that control systems cyber security is critical to the corporate goal of operational safety.

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

## Recommendations for Government Leadership Priorities

The Working Group found strong and committed government efforts underway 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 best address the cyber threat to control systems.

### Recommendations:

- 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) to evaluate each sector's strategy to meet the national control system survivability goal set for 2015.
- 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.
- DHS work with the Malcolm Baldrige Award for Excellence in Business Management and/or other similar programs to help communicate the importance of control systems cyber security to business leaders.

10

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

## Recommendations for Improved Information Sharing

The Working Group 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.

### Recommendations:

- DHS enhance the control system cyber incident information collection mechanism at Carnegie Mellon's CERT Coordination Center (CERT/CC) for collection, protection, and sharing.
- DHS rapidly ramp up CERT/CC's support services for control system operators to help develop a cyber incident information collection capability.
- The Office of the Director of National Intelligence (DNI) develop a solution to the problem of originator control (ORCON) that currently prevents DHS from sharing threat information with critical infrastructure operators.
- 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.
- DHS share relevant information from the Threat Assessment and NIE with critical infrastructure control systems operators.

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

## Recommendations for Improved Information Sharing *(continued)*

- 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 on threats, CERT/CC and other sources on incidents, and DHS (including US-CERT) on cyber vulnerabilities.
- DHS will communicate resulting warning information to control systems owner-operators to ensure protection of U.S. critical infrastructures.
- The Program Manager, Information Sharing Environment, include information on control systems cyber threats in the Information Sharing Environment (ISE).

12

NIAC WORKING DRAFT—NOT FOR REDISTRIBUTION

## Next Steps

---

- ▣ Full Council consideration/approval of the Final Report and Recommendations.
- ▣ Deliver NIAC Final Report and Recommendations to the President.

## Discussion

---

- ▣ Questions?