National Infrastructure Advisory Council (NIAC)

Convergence Working Group

Status Report
October 10, 2006

George H. Conrades
Executive Chairman
Akamai Technologies

Greg Peters
Managing Partner
Collective IQ

Margaret Grayson
President, Grayson and Associates

Overview

- Purpose
- Status of *Next Steps* from Last Meeting
- Timeline
- Actions
- Directional Recommendations
- Next Steps

Purpose

- Mission: The Convergence Study Group will investigate important questions and make recommendations regarding the protection of SCADA and Process Control Systems from cyber threats.

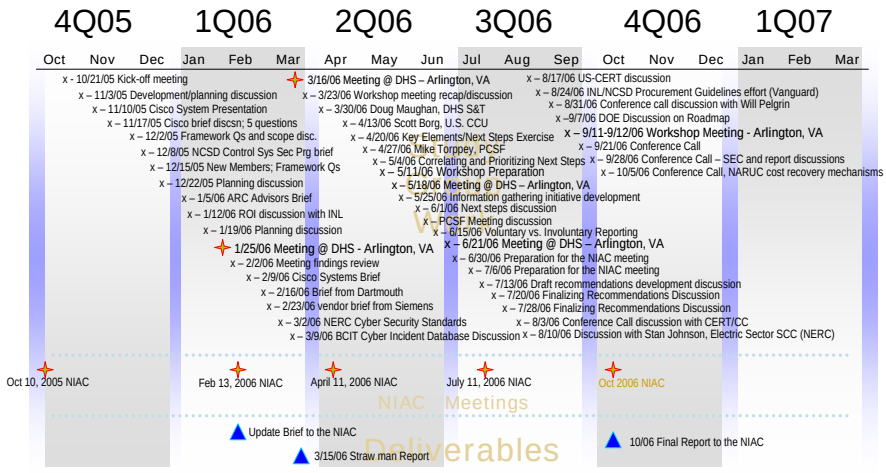
Process: The Five Framework Questions

- ***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?

Status of *Next Steps* from Last Meeting

- ✓ Investigated outstanding key elements, developed two more directional recommendations
- ✓ Provided Malcolm Baldridge Award board of overseers appropriate criteria for control systems cyber security to increase awareness of cyber security threat to control systems
- ✓ Collected input from executives and subject matter experts to refine directional recommendations
- ❑ Validate and strengthened recommendations before finalizing
- ❑ Draft the final report incorporating additional information underlying actionable recommendations for a Final Report to be submitted to the NIAC for the January meeting

Time Line



Actions

- Held 13 more (total of 41 to date) weekly conference call discussions with subject matter experts to validate the findings and potential recommendations
- Held 4th face-to-face workshop to develop the draft findings and recommendations.
- Developed draft findings and draft report

Directional Recommendations

- **Security as an Enabler:**
  The study group found that executive leadership awareness and information sharing are critical to achieving a culture in control systems operators where security is valued as inseparable from availability, reliability and safety goals.
- **Market Drivers:**
  The study group found insufficient market drivers to achieve industry attention and focus for control systems security product/systems development and implementation in some sectors.
  - To ensure appropriate measures are present in each sector, the Study Group suggests that the Working Group recommend that the framework outlined in the *NIAC Best Practices for Government to Enhance Security of the National Critical Infrastructures* be applied by each Sector Coordinating Council to their respective sectors with regard to improving control systems cyber security. Outcomes should be validated by the corresponding Sector Specific Agency, and results reported to DHS through existing mechanisms.

Directional Recommendations

- **Executive Leadership Awareness:**
  The Study Group found that executive leadership awareness of the cyber threat to control systems, across private sector and government sector control systems operator and vendor, is critical to achieving all needed action.
  - To improve executive leadership awareness of the cyber threat to critical infrastructure control systems, the Study Group suggests the Working Group recommend that a detailed approach to communicate the cyber threat to control systems be applied by DHS to executive leaders in the critical infrastructure sectors, government and the vendor community.
  - To communicate strategic threat information to executive leaders, the Study Group suggests that the Working Group recommend that DHS establish communication processes for this information through the Sector Coordinating Councils (SCCs) to reach control systems owner-operators in a reliable and protected manner.
  - To effectively communicate the executive awareness outreach message, communications should use the risk self-discovery approach developed by the US-CCU and include strategic level information on threats, hostile actors, economic motivators for hostile actors, consequences.

Directional Recommendations

- **Government Leadership:**
  The Study Group found that integrated coordination and planning among committed government efforts for addressing the cyber threat to control systems will substantially reduce the dynamic nature of this threat.
  - Establishing a public/private partnership to increase executive awareness, the Study Group suggests that the Working Group recommend collaborating with the Malcolm Baldridge Award for Excellence in Business Management to communicate the SCADA/PCS cyber security message to business leaders.
  - The Study Group suggests that the Working Group recommend that federal government funding for control systems security R&D is coordinated based on priorities identified by Cyber Security and Information Assurance Interagency Working Group (CSIA IWG) annual reports using the President's recently established cross-cut process to prioritize cyber R&D funding in the Presidents Budget submitted to Congress.

Directional Recommendations

- **Government Leadership:** *(continued)*
  - The Study Group suggests that the Working Group recommend appropriate focus and funding for development of DHS's Control Systems Security Program's (CSSP) security tools, including the Vulnerability Assessment Tool (VAT).
  - The Study Group suggests that the Working Group recommend that federal government agencies use the Procurement Language for Control Systems Security document when procuring control systems and services, when applicable.

Directional Recommendations *(continued)*

- **To Improve information sharing:**

  The Study Group found that improved information sharing is critical to a properly informed and measured response to the threat to critical infrastructure control systems.
  - For improved understanding of the threat to control systems and more accurate risk assessment decisions, the Study Group suggests that the Working Group recommend collection of cyber incident data through Carnegie Mellon's CERT Coordination Center as a trusted and protected third party mechanism for collection, protection, and appropriate dissemination of aggregated incident information.
  - To improve both the available resources for companies seeking to address the cyber vulnerabilities to their SCADA and PCS systems, the Study Group suggests that the Working Group recommend that CERT/CC be provided with the necessary resources to rapidly ramp up their SCADA/Process Control Systems training and engineering consulting services needed to build the trusted relationships that will facilitate incident information sharing.

Directional Recommendations *(continued)*

- To Improve information sharing *(continued)*:
  - To improve sharing of strategic threat information, the Study Group suggests that the Working Group recommend that a formal Request For Information (RFI) be submitted by the White House to the intelligence community to assess the cyber threat to SCADA and Process Control Systems, so that this vital information can be communicated to critical infrastructure owner-operators to better inform strategic risk assessments for their systems.
  - To Improve information sharing and get the right information to the right people at the right time, the Study Group suggests that the Working Group recommend that information on control systems cyber threats be integrated/included in the forthcoming Congressionally-mandated and President-directed Information Sharing Environment. This robust protected information sharing mechanism will increase the visibility and usefulness of this critical information.

Next Steps

- Investigate opportunities for cross sector applicability of the recommendations to manage the risks of convergence of cyber/physical control systems environments
- Complete documentation of findings and recommendations, including some further discussions with affected agencies and entities
- Further refine directional recommendations as actionable, measurable and accountable
- Finalize Report and submit to the NIAC

Discussion

- Questions?