

*Keep America Working:  
Developing Secure Digital/Electronic Process Control Systems  
For the Nation's Critical Infrastructures  
Draft*

**National Strategy Meeting  
9:00 am—4:00 pm  
2 April 2002  
U.S. Department of Commerce**

*Conference Highlights*

Prior to 9/11 national economic security focused mainly on export controls and free trade. Today, however, national economic security requires a functional economy during and after a terrorist attack. This requires consumer and economic confidence, which can only be maintained with the cooperation and collaboration of the private sector. With government as a facilitator rather than a regulator, users and makers of digital control systems must do their part to address vulnerabilities to enhance national economic security. Industry has a role and responsibility to make security and security awareness part of business operations and planning in their own vested interests.

Rules have changed. Now, when we know about vulnerabilities that may be subject to possible terrorist exploitation, the federal government, the private sector, and all Americans must seek to fix them. It is in industry's long-term economic interest to fix vulnerabilities now—rather than suffer the consequences. The aviation industry continues to feel the effects of more regulation, a new Transportation Security Agency, Congressional bailouts, and even bankruptcy.

Presidential Executive Order (13231) established the President's Critical Infrastructure Protection Board (PCIPB). This order emphasizes the degree to which the IT Revolution has changed the nature of the American economy, and calls for an industry-government partnership to help secure critical infrastructures using market forces.

Towards this end, the President has asked for a national strategy to secure cyberspace; in that strategy, the government seeks a roadmap on how best to secure digital control systems that underpin this nation's critical services: how should it be done? More awareness? With more encryption? Industry best practices? More research? While there is little doubt that the lines between "physical" and "cyber" security continue to blur, it is clear that digital control systems are organizational key elements that run through all parts of critical service operations.

The goal of today's conference is to start drafting this roadmap under the partnership rubric. The conference hopes to promote collaboration, identify current work that is being done, identify gaps, and propose recommendations for government involvement and improvement.

*Keep America Working:  
Developing Secure Digital/Electronic Process Control Systems  
For the Nation's Critical Infrastructures*

*Working Group Breakout Session 1:  
User Requirements and Needs*

**Priority Areas of Consideration**

1. Industry needs a "Top 10 Checklist" highlighting easy-to-fix, high return initiatives.
2. There need to be security "roles" and "priorities" for industry and government for the short-term, medium-term, and long-term.
3. The security awareness and education of corporate CEOs should be increased through development of a Business Case for Action with identified threats baselined.
4. Security guidelines and specifications should be issued to vendors.
5. Guidance and specifications for governance (e.g., policy, procedures, plans and training guidance) should be developed.
6. Threat awareness and identification should be increased for the public at-large.
7. Cross-sector best practices should be developed and shared.
8. The barriers to information sharing, such as FOIA, need to be considered and solved.

**Other Points to Consider**

- NIST has a Process Control Security Requirements Forum (PCSRF) for utilities and manufacturing, with the objective of developing a protection profile for control systems.
- The Open Group's Active Loss Prevention Program Secure Systems Methodology cuts across sectors.
- The Business Case for Action needs to reflect cost outside of the infrastructure itself (to customers of the infrastructure).
- Diverse threats strain resources, and multiple messages from different Federal entities are causing confusion. Industry needs to have target prioritization information.

***In addition to the points discussed above, five specific areas should be considered:***

*Keep America Working:  
Developing Secure Digital/Electronic Process Control Systems  
For the Nation's Critical Infrastructures*

- Industry needs to tell the government how to foster security awareness at the CEO and the Corporate Board level. In addition, security awareness at the employee level should be enhanced. One idea is to create a "Security Game" that employees "play" before gaining system access.
- Industry should use a vulnerability paradigm, rather than a threat paradigm, when addressing and thinking about security. Access to threat information will not solve industry problems, because you will not know about threats in advance. Industry should assess vulnerabilities, factor them, and develop a prioritized list.
- Industry should help government direct R&D expenditures and priorities. Government needs to know first that industry wants more research, and then specifically what areas need concentration.
- Industry should help government develop security standards; this could be done in conjunction with NIST.
- Industry should provide input to the National Strategy to Secure Cyberspace, which will come out this summer. Any input to the government should be delivered by the end of June, 2002.

*Working Group Breakout Session 2:  
DCS/Security Technology Directions/R&D/Standards*

**Priority Areas of Consideration**

1. There needs to be a mechanism for information sharing within and across sectors. When and where appropriate, this information sharing resource must protect the sensitivity/identity of the information it receives. Further, government needs to clarify how Sensitive But Unclassified (SBU) information can and should be shared across sectors. This information sharing mechanism should also include a means to exchange R&D.
2. There needs to be a "test-bed" to conduct reality bases scenario experimentation where industry and government can explore vulnerabilities and potential fixes. For example, if cyber-terrorists attack a power grid, how will the grid *actually* respond? How much damage will the attack cause and what type of damage? Will there be measurable cascading effects? This "test-bed" can also serve as a showcase to display security expertise.
3. There should be a standardized threat and security template that will allow each user to conduct threat and vulnerability assessments.
4. There needs to be increased coordination among parties working on security issues across various industries and sectors.
5. Government and industry should review the underlying security assumptions that form the basis for security standards, including the consequences if those assumptions are invalid.

*Keep America Working:  
Developing Secure Digital/Electronic Process Control Systems  
For the Nation's Critical Infrastructures*

6. Government needs to provide seed money for R&D as well as an R&D mandate. There also needs to be economic incentives to aid security deployment.
7. Industry needs to understand the motivation for deploying secure systems (i.e. increased awareness). Can there be economic security motivators, such as tax credits or accelerated depreciation allowances?
8. There need to be security awareness and education campaigns so users and manufactures understand security issues. There should be a consistent way to express industry best practices.
9. Business should incorporate security considerations across a product's life cycle.

**Other Points to Consider**

- The industry understands safety in clear terms; it is logical to make security “look like” and “sound like” safety.
- What is the extent of private security initiatives currently underway? Can these initiatives be incorporated into this national framework?
- There should be increased cooperation and coordination among sector working groups and workshops. This will promote knowledge sharing and help identify mutual areas of concern across sectors.
- Outside expertise should be utilized, where appropriate. This might include the national labs or private corporations.
- Use lessons learned from Y2K, especially with regard to national awareness and consumer marketing.
- Industry should consider teaming more closely with IEEE to write security standards.
- There is a loss of human “security” capital. Industry needs to educate and re-educate the workforce with regard to information security.