



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

Walk the Talk: How PNNL is Adopting a Supply Chain Security Culture

GRETCHEN HUND

Director, PNNL Center for Global Security

Presentation to Export Control Coordinators Organization (ECCO)

April 20, 2016

Agenda



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

- ▶ Goal
- ▶ Background
- ▶ Principles of Conduct
 - Opportunities for action
 - PNNL activities
 - Feedback from senior staff
 - Next steps
- ▶ Lessons Learned
- ▶ Conclusion



Background

- ▶ Conducted industry interviews as part of NNSA self-regulation project to encourage companies to adopt internal best practices
- ▶ Reviewed companies' responses to 'beyond compliance' measures
- ▶ Companies acknowledged the responsibility to secure goods and services throughout their supply chain

If companies are being asked to consider adopting these best practices, shouldn't we "walk the talk?"

Opportunities for Action



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

Walk the Talk: Supply Chain Security

1. Corporate governance
2. Principles of Conduct
3. Training
4. Contracting
5. Technology commercialization and transfer
6. Export control
7. Participation in government rulemaking
8. Messaging and reporting



1. PNNL Corporate Governance

- ▶ Emphasize our commitment to achieving excellence in controlling and securing our supply chain
 - Set expectations to ensure sensitive goods and information do not end up in the wrong hands
 - Within our core value of Integrity, consider adding:
 - *Ensure a strong commitment to excellence in managing our operations and our supply chains to protect sensitive goods and technology*
- ▶ Operational examples:
 - Define and include Export Control under information release platforms
 - Improve screening questions for “export,” “international,” and other terms to better define supply chain security risks in setting up projects



2. Principles of Conduct

1. Adopt and communicate a corporate governance statement on supply chain security.
2. Participate in relevant supply chain security codes of conduct or pledges.
3. Preferentially select business partners that maintain strong supply chain security practices.
4. Incorporate supply chain security concepts into employee training and education to promote a supply chain security culture.
5. Require that all presentations given and papers written do not transfer sensitive information without appropriate authorization.
6. Include supply chain security requirements in technology commercialization and transfer processes.
7. Participate in governmental rulemaking related to supply chain security, such as export requirements and procurement flow-down requirements for subcontractors.
8. Develop a corporate policy on reporting anomalous incidents to appropriate parties.



3. Training and Education

- ▶ Make trainings memorable for employees through visual learning and highlight supply chain security through education materials
 - Include a short, supply chain security training module (highlight export control, foreign travel, conferences, ethics, counterintelligence, etc.), including on information release platforms and export control determinations
 - Develop “Lessons Learned” with real security examples illustrating how small actions can jeopardize national security interests



🌟 Staff members practice situational awareness to avoid potentially classified conversations

Date Published: March 8, 2016 | Contact: HDI POC - Security | [Read Comments \(0\)](#)

Staff members used their training to stop discussions and protect potentially sensitive information

Summary

In two recent situations, PNNL staff members recognized that potentially classified or sensitive conversations may be occurring with individuals who do not work for the Lab. The staff members practiced situational awareness and used their training to recognize they needed to exit the conversations, report the

issues to their managers, and call PNNL's Single Point of Contact. **Lessons Learned:** PNNL staff members are trained to react to potentially classified or sensitive conversations by utilizing the "no comment" policy, not confirming technical accuracy,





4. Contracting

- ▶ Define and implement selection criteria for supply chain security in bidding/procurement practices
 - As appropriate, preferentially procure from and subcontract with companies that maintain strong supply chain security programs
 - Provide opportunity for RFP bidders to explain how they implement supply chain security and export controls in daily operations
 - Include language in RFPs and SOWs that clearly state PNNL supports and values supply chain security
 - Ideally give credit to entities that are more transparent in sharing their practices through “best values” evaluation criteria
 - Apply flow down requirements where appropriate
 - Engage ECO in defining selection criteria



5. Technology Commercialization & Transfer

- ▶ Include supply chain security requirements in technology commercialization and transfer processes
 - In vetting companies, determine the robustness of their supply chain security program
 - Do they follow these best practices?
 - Do they have an internal compliance program?
 - Material transfer agreements to include strict limitations on use and dissemination, beyond exclusive license agreements
- ▶ Have checks in place to monitor third-party sub-licensees
 - Expand language to prevent information release about non-desired or sensitive uses
 - Consider approaches (e.g., audits) to ensure that licensees get laboratory approval before issuing a sub-license (even for non-exclusive licenses)
- ▶ Consider having ECO review technology prior to having the U.S. Patent Office do the review



6. Export Control

- ▶ Require that presentations and papers written for external audiences do not transfer sensitive information
 - Implement appropriate operation controls throughout lab
 - Conduct a risk determination including export control in our project set-up system and include it in our newly revised information release platform
- ▶ Long-term goal: Establish Supply Chain Security Working Group
 - Evaluate our progress in meeting principles — members could include Export Control Office, general counsel, contracts, training, counterintelligence, appropriate risk review managers, tech commercialization/transfer
 - Develop metrics to measure performance



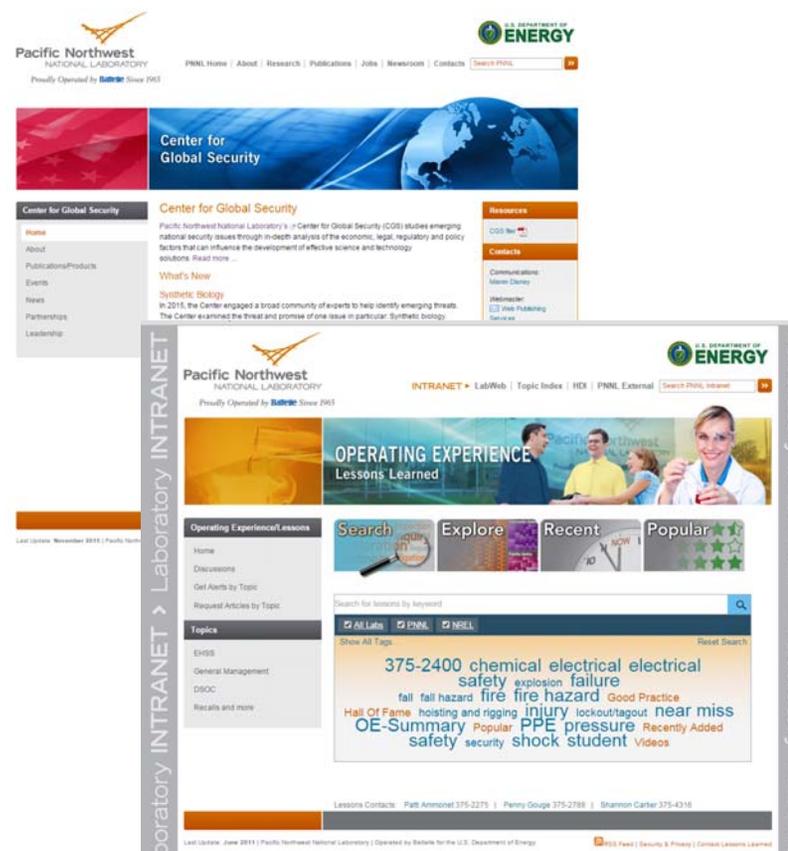
7. Participation in Government Rulemaking

- ▶ Increased industry-government information sharing can result in better-informed and more-efficient regulation
- ▶ PNNL has provided comments. Examples:
 - NNSA's revision of the Code of Federal Regulations Title 10 Part 810, which controls the export of unclassified nuclear technology and assistance
 - DOC/BIS proposes a rule revising Supplement No. 1 to Part 766 of the Export Administration Regulations, Guidance on Charging and Penalty Determinations in Settlement of Administrative Enforcement Cases.



8. Messaging and Reporting

- ▶ Broaden public messages to emphasize supply chain security
- ▶ Update communication materials and website content
- ▶ Encourage major partners, including governmental agencies and other national laboratories, to adopt similar measures (beginning with ECCO)
- ▶ Report regularly on developed supply chain security metrics





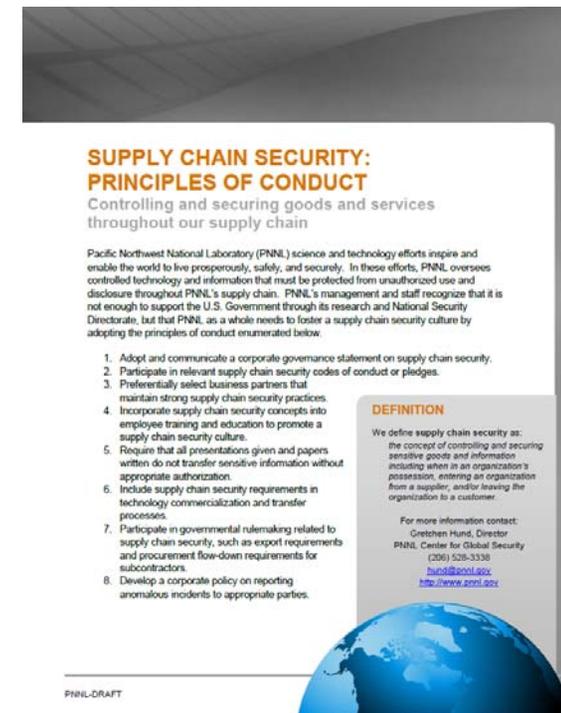
Lessons Learned for Adopting Principles

- ▶ Multiple laboratory parties involved:
 - *Export Control*
 - *Legal*
 - *Counter Intelligence*
 - *Contracts*
 - *Technology Commercialization*
 - *Senior Managers, M&O Program Managers, Research Operations Council*
 - *Training*
 - *Communications*
- ▶ Easiest Lift: Communications (i.e., lessons learned, flyers, brown bags)
- ▶ Hardest Lift: Coordinating all of the parties and demonstrating the value added
- ▶ Communicate consequences of not “Walking the Talk”
 - Can Lab leaders adequately support the identified areas to help engrain a supply chain security culture and secure PNNL’s supply chain?

Conclusion

- ▶ All government institutions should consider “Walking the Talk” in supply chain security by adopting best practices
- ▶ Adopting recommended best practices can be both easy and challenging
- ▶ Important to share lessons learned
- ▶ What more could your institution do to “Walk the Talk”?

***Thank you.
Gretchen Hund
Director, Center for Global Security***



Draft Principles of Conduct