



**Pacific Northwest**  
NATIONAL LABORATORY

*Proudly Operated by Battelle Since 1965*

# Walk the Talk: Progress in Building a Supply Chain Security Culture

## Annual Update

### August 2016

G Hund

## DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights.** Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY  
*operated by*  
BATTELLE  
*for the*  
UNITED STATES DEPARTMENT OF ENERGY  
*under Contract DE-AC05-76RL01830*

Printed in the United States of America

Available to DOE and DOE contractors from the  
Office of Scientific and Technical Information,  
P.O. Box 62, Oak Ridge, TN 37831-0062;  
ph: (865) 576-8401  
fax: (865) 576-5728  
email: [reports@adonis.osti.gov](mailto:reports@adonis.osti.gov)

Available to the public from the National Technical Information Service  
5301 Shawnee Rd., Alexandria, VA 22312  
ph: (800) 553-NTIS (6847)  
email: [orders@ntis.gov](mailto:orders@ntis.gov) <<http://www.ntis.gov/about/form.aspx>>  
Online ordering: <http://www.ntis.gov>



This document was printed on recycled paper.

(8/2010)

# **Walk the Talk: Progress in Building a Supply Chain Security Culture**

G Hund

August 2016

Prepared for  
the U.S. Department of Energy  
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory  
Richland, Washington 99352

# Contents

1.0 Overview .....	1
Appendix A Walk the Talk Flyer.....	A.1
Appendix B Walk the Talk Presentation to the ROC .....	B.1
Appendix C Walk the Talk Lessons Learned .....	C.1

# 1.0 Overview

Pacific Northwest National Laboratory (PNNL) has engaged industry to “go beyond compliance” for over a decade in controlling and securing their supply chains to ensure their goods are not diverted to nuclear weapons programs. This work has focused on dual-use industries that manufacture products that can be used in both commercial applications and in the development of a nuclear weapon. The team encourages industry to self-regulate to reduce proliferation risks. As part of that work, PNNL interviewed numerous companies about their compliance practices to understand their business and to build awareness around best practices to ensure security of goods, technology, and information along their supply chains.

From conducting this work, PNNL identified indicators that a company can adopt as part of its commitment to nonproliferation ideals with a focus on supply chain security. The indicators were updated this past year and are described in detail in the flyer featured in Appendix A. They include:

1. Adopt and communicate a corporate governance statement on supply chain security
2. Participate in relevant nonproliferation codes of conduct or pledges
3. Preferentially select business partners that maintain strong supply chain security practices
4. Develop a corporate policy on reporting anomalous incidents to appropriate parties
5. Include supply chain security requirements in technology commercialization and transfer processes
6. Participate in governmental export control rulemaking
7. Incorporate supply chain security concepts into employee training/education
8. Require that external communications do not transfer sensitive information without appropriate authorization.

Believing that national laboratories should follow these same best practices, the team has been leading an effort to help laboratories “walk the talk,” starting at PNNL. The team is working to implement a lab-wide supply chain security program, including promoting a supply chain security culture, similar to that which has been developed for safety. Adopting a supply chain security culture means that numerous operations and departments at the lab are being made aware of the importance of supply chain security.

The lead for this effort, Gretchen Hund, met with senior PNNL representatives in contracts, legal, export control, counter-intelligence, technology commercialization, training, and communications to describe the concept and to discuss the steps required to implement a supply chain security program so that PNNL could more cohesively “walk the talk.” After meeting with the department leads, it was clear that PNNL is already doing much of what is necessary (as captured in the attached flyer) but that more can be done to fully embrace the culture and to build awareness and engagement among lab staff.

Ms. Hund had a follow-up meeting with PNNL’s Research Operations Council (ROC), which represents operations from across the laboratory, on March 15, 2016. The ROC members requested that Ms. Hund further define the costs associated with implementing Walk the Talk and the envisioned benefits. They supported the presentation she planned to make at the Export Control Coordinators Organization annual meeting the following month (April 18, 2016) with the export control leaders from across the national laboratory complex. The presentation is available in Appendix B. Ms. Hund ended her presentation with the flyer showing the eight principles she was encouraging other laboratories to follow.

Two national laboratories, Los Alamos National Laboratory and Kansas City Plant both indicated they wanted to be part of Walk the Talk.

The Walk the Talk team developed a breakdown of all of the tasks necessary to meet the intention of each of the eight principles and the costs and envisioned benefit associated with each of them. Meetings were held with operations staff responsible for various activities. For example, the team met with the team that is updating the information review and release process for all documents to identify further checks and balances across the laboratory, not just the National Security Directorate, to ensure that sensitive information is not released. The team also met with the Communications *Lessons Learned* staff and together developed a *Lessons Learned* that is posted on the PNNL internal website for all staff to view (see Appendix C), and it was featured in a weekly wrap-up of the National Security Directorate's Chief Operating Officer and on the internal *Inside PNNL* news publication. This *Lessons Learned* used the recent Alan Ho case as an example of how staff can be recruited to share sensitive information. This is an example of a "don't let this happen to you" story.

Moving forward, the PNNL team will continue working with PNNL leaders to promote more widespread and visible adoption of the supply chain security culture, to the extent permitted by laboratory managers. The team will continue to fill in the task matrix of steps necessary to endorse each of the principles and estimate the cost and benefit associated with them. The team will work to incorporate the supply chain security principles across all elements of the laboratory. The PNNL team will continue sharing PNNL's "walk the talk" initiative at various venues and continue to engage other laboratories.

## **Appendix A**

### **Walk the Talk Flyer**



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

Pacific Northwest National Laboratory (PNNL), in support of the U.S. Department of Energy (DOE), oversees controlled technology and information and needs to protect these valuable assets with a strong supply chain security culture. We recognize that it is not enough to support the U.S. Government through nonproliferation program work—we need to “walk the talk” in our daily operations. The table below illustrates how PNNL is adopting Principles of Conduct to foster a culture of supply chain security.

Supply Chain Security Indicator	PNNL Walking the Talk
1. Adopt and communicate a corporate governance statement on supply chain security	PNNL proposed Principles of Conduct to complement our corporate governance, therein bolstering supply chain security efforts: Our vision is “PNNL science and technology inspires and enables the world to live prosperously, safely, and securely;” Battelle’s is similarly guided by a shared belief that “no business objective is worth achieving at the expense of our integrity and ethics.”
2. Participate in relevant nonproliferation codes of conduct or pledges	No explicit nonproliferation code of conduct exists at PNNL nor does one currently exist among National Laboratories. To address this gap, PNNL developed Principles of Conduct to support supply chain security and is communicating them to build awareness inside and outside the laboratory.
3. Preferentially select business partners that maintain strong supply chain security practices	In sole-source contracts, PNNL can require a contracting entity to have supply chain security controls in place. PNNL is exploring avenues to include language in relevant Request for Proposals and Scopes of Work and to enhance selection criteria that strengthen supply chain security practices in bidding and procurement processes.
4. Develop a corporate policy on reporting anomalous incidents to appropriate parties	Mandatory staff training includes being alert for individuals who may attempt to gather sensitive information and reporting unusual/suspicious requests or suspicious activities.
5. Include supply chain security requirements in technology commercialization and transfer processes	Patents are drafted with supply chain security interests in mind. The Export Control Office reviews the technology prior to a license being considered. The commercialization team verifies that candidate licensees have supply chain security measures. Other measures such as exclusive licenses and flowdown requirements ensure greater oversight on commercialization and transfers.
6. Participate in governmental export control rulemaking	PNNL supports U.S. agencies in rulemaking, such as supporting the National Nuclear Security Administration’s revision of the Code of Federal Regulations Title 10 Part 810, which controls the export of unclassified nuclear technology and assistance, and commenting on the Department of Commerce’s proposed 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.
7. Incorporate supply chain security concepts into employee training/education	All PNNL staff (including interns and contractors) complete mandatory training that includes export control and defines the importance of protecting all sensitive information, technology, and equipment.
8. Require that external communications do not transfer sensitive information without appropriate authorization	PNNL National Security Directorate material planned for release is reviewed by a Derivative Classifier and content planned for foreign distribution is also reviewed by a trained export control office staff member. We are revising our Information Release and Electronic Prep and Risk processes to better address export control sensitivities and information determinations.

PNNL is at the forefront of developing solutions to stop the spread of weapons of mass destruction. The laboratory is taking additional efforts to make nonproliferation a mainstay of our operations as well as sharing our proposed Principles of Conduct as a possible model for others. Our researchers present on the subject of integrating nonproliferation into corporate sustainability and on building and maintaining a culture around supply chain security at national and international meetings.

## WHAT'S NEXT?

A strong supply chain security culture means avoiding complacency. PNNL continues to explore opportunities to continuously improve supply chain security by:

- » More explicitly weaving supply chain security into our corporate governance statement so our stakeholders clearly understand this commitment to adopt the eight Principles of Conduct at the corporate level.
- » Implementing robust selection criteria for supply chain security practices in bidding/procurement processes.
- » Incorporating lessons learned into training and periodic lab-wide publications to convey the importance of controlling and securing information, technology, and equipment at all times and in all activities. This includes promoting behavior expectations for staff at conferences and other venues.
- » Requiring all presentations and papers be reviewed by the appropriate manager and, when necessary, the Export Controls Office to ensure no sensitive information is included.
- » Helping partners and sponsors adopt similar measures within their supply chains, potentially adopting PNNL's Principles of Conduct.

PNNL is committed to measuring progress toward meeting these metrics and to work with others to grow and maintain a supply security culture.

## Where did the eight Principles of Conduct come from?

In 2013, research staff at PNNL published an article defining numerous indicators for a strong supply chain security culture. PNNL has since translated the indicators into the principles of conduct and outlined tangible metrics that will allow our organization to track and report on our progress more regularly. Entities that adopt similar metrics can more transparently report on their activities, enabling regulators, investors, employees, and the general public to understand how they are going beyond compliance and are committed to a more sustainable and secure supply chain.

Reference: Kurzrok AJ, and G Hund. (2013). "Beyond compliance: Integrating nonproliferation into corporate sustainability." *Bulletin of the Atomic Scientists*. 69:31. DOI: 10.1177/0096340213485946.



### Contact:

**Gretchen Hund**

Director, Pacific Northwest Center for Global Security  
Pacific Northwest National Laboratory  
Tel: 206-528-3338 | hund@pnnl.gov



**Pacific Northwest**  
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965

## **Appendix B**

### **Walk the Talk Presentation to the ROC**



**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

- ▶ 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?"**



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

**OPERATING EXPERIENCE**  
Lessons Learned

★ 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



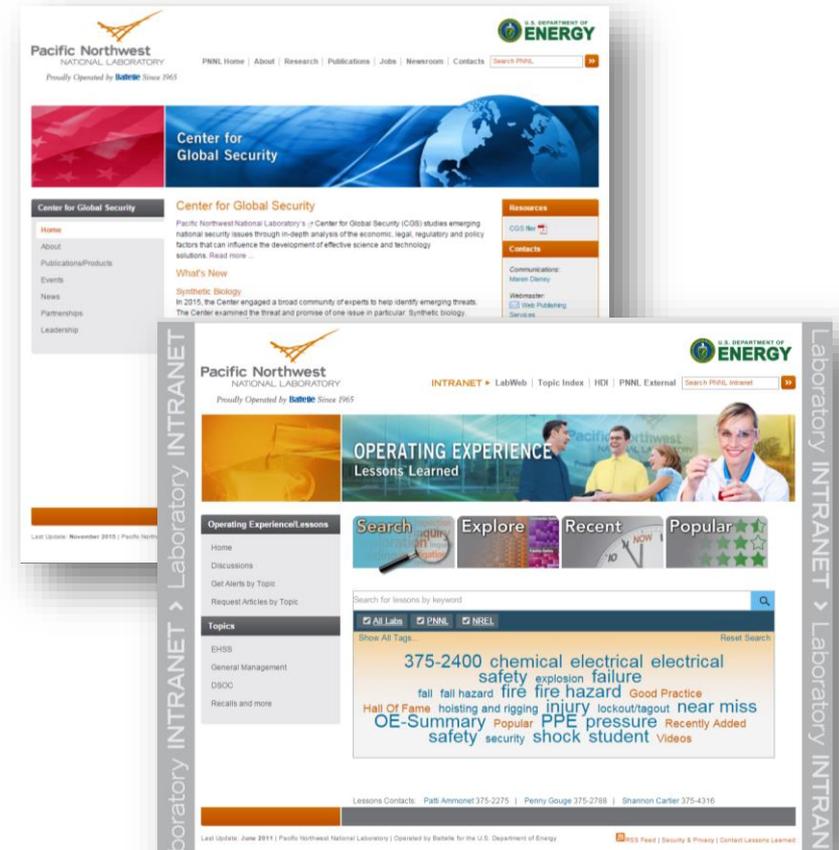
## 7. Participation in Government Rulemaking

- ▶ 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***

**SUPPLY CHAIN SECURITY:  
PRINCIPLES OF CONDUCT**  
Controlling and securing goods and services throughout our supply chain

Pacific Northwest National Laboratory (PNNL) science and technology efforts inspire and enable the world to live prosperously, safely, and securely. In these efforts, PNNL oversees controlled technology and information that must be protected from unauthorized use and disclosure throughout PNNL's supply chain. PNNL's management and staff recognize that it is not enough to support the U.S. Government through its research and National Security Directorate, but that PNNL as a whole needs to foster a supply chain security culture by adopting the principles of conduct enumerated below.

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.

**DEFINITION**

We define supply chain security as:  
*the concept of controlling and securing sensitive goods and information including when in an organization's possession, entering an organization from a supplier, and/or leaving the organization to a customer.*

For more information contact:  
Gretchen Hund, Director  
PNNL Center for Global Security  
(206) 528-3338  
[hund@ornl.gov](mailto:hund@ornl.gov)  
<http://www.pnnl.gov>

PNNL-DRAFT

Draft Principles of Conduct

## **Appendix C**

### **Walk the Talk Lessons Learned**



## Supply chain security: How PNNL is adopting enhanced security for sensitive information

Date Published: August 1, 2016 | Contact: [HDI POC - Security](#) | [Read Comments \(0\)](#)

***All staff members are responsible for protecting information and watching for suspicious activity***

### Summary

Anyone in the national laboratory supply chain, from researchers to executives to subcontractors, can be targets for espionage. Nuclear Engineer Allan Ho enlisted six U.S.-based nuclear experts, including a senior manager in the Tennessee Valley Authority's (TVA) nuclear program, to supply information on nuclear outage and fuel data. Ho and others were ultimately arrested for passing information on U.S. nuclear programs to Chinese-owned firms, marking the nation's first nuclear espionage conspiracy case involving China. **Lessons**

**Learned:** As a staff member of a national laboratory, you could be targeted and approached by individuals who want access to information you possess. Be vigilant and report any concerns or observations to your manager, PNNL's Single Point of Contact, or the legal department. To help raise security awareness, PNNL's Center for Global Security is actively sharing "supply chain security" guidance, sharing behaviors and best practices that can be implemented across all levels of the organization and externally with other national laboratories, suppliers, and stakeholders. The Center helps ensure we are "walking the talk" in protecting knowledge, technology, and components at all times, both locally and abroad.



### The Nuclear Espionage Case

Prosecutors say Allan Ho's conspiracy began in 1997 and continued until his arrest with the intent to help advance China's nuclear industry. Ho was born in Taiwan, educated in the United States, and is a naturalized citizen. He was arrested in April for passing nuclear information to China, along with recruiting six U.S.-based nuclear experts to supply technical information to one of China's largest nuclear power companies. One of the experts Ho paid for information was an unidentified senior engineer who was employed by the Tennessee Valley Authority (TVA) nuclear program from 2010-2014. Prosecutors have declined to say whether the six experts Ho recruited are being prosecuted or have struck deals to cooperate with the investigation. Ho's trial is set for January 2017.

PNNL's Center for Global Security is actively sharing "supply chain security" guidance to raise awareness to the potential for targeting such as that accomplished by Ho. The Center is also focused on fostering behaviors and best practices that can be implemented across all levels of the organization and externally with other national laboratories, suppliers, and stakeholders to better protect knowledge, technology, and components at all times, both locally and

abroad.

## What is Supply Chain Security?

"Supply chain security" is the concept of controlling and securing sensitive goods and information along the whole supply chain, including when in an organization's possession, entering an organization from a supplier, and/or leaving the organization to a customer. PNNL's Center for Global Security developed eight [Principles of Conduct](#) to foster a strong security culture through controlling information and enabling behavior change through training and education. If the organizations and individuals involved in the Ho case were following these principles, the targeted information may not have been released.

Although initiated to raise awareness within the international nuclear industry community, this work is also focused on ensuring that PNNL and the other DOE labs "walk the talk." As global concerns evolve, supply chain security culture is expanding beyond nuclear nonproliferation to include emerging national security concerns in many other areas including nuclear, radiological, biological, chemical, and cybersecurity. The focus is on anything that can be used in developing a weapon of mass destruction.

## Why is Supply Chain Security Important to PNNL and to You?

YOU are part of the PNNL supply chain! Do you travel on PNNL business or attend conferences? Do you deliver presentations or materials related to Lab business? Do you work with colleagues from other countries or international organizations both while in the United States and abroad? These are but a few situations when information or research you possess could be compromised. With work in the nuclear, radiological, chemical, biological, cyber arenas, PNNL staff may attract individuals with nefarious intentions. The espionage case against Ho is a reminder that others may want access to information or materials involving PNNL work.

The FBI reports a marked increase in cases of economic espionage, spear phishing, and theft of intellectual property being directed by foreign governments. "The arrest and indictment in the Allan Ho case sends an important message to the U.S. nuclear community that foreign entities want the information you possess," says FBI Executive Assistant Director Michael Steinbach. "This can result in significant damage to our national security." The FBI's message underpins the reminder that, as staff members of a national laboratory, you may be a target for those who want information you work with or can access so a questioning attitude is critical.

## Lessons Learned

Supply chain security applies to the entire Lab. Safeguarding information entrusted to us as a national lab applies to any of our work that can be used nefariously. All staff members have a responsibility to protect the Lab's information assets and to remain vigilant about suspicious activity. Maintaining excellence in supply chain security differentiates PNNL as a national laboratory and business partner and can be an advantage when competing for work.

### All Staff

- **Consider how supply chain security pertains to your role.** We can all contribute to supply chain security by controlling and securing sensitive information, technology, and equipment at work and on travel. Become familiar with and use appropriate [OPSEC countermeasures](#) to protect sensitive information and technology.
- **Assure presentations and materials are reviewed by Export Control.** Have presentations and papers for delivery to external audiences, including materials for foreign distribution, reviewed by Export Control prior to delivery. See the [Export Control](#) web page for more information.
- **Be aware of protecting information when traveling or at conferences.** Remain alert to where you are viewing Lab information on a laptop or tablet. Electronics within eyesight of others on airplanes or left in hotel rooms may be a target. Conference attendees may attempt to lure Lab staff members into sharing information without thinking about the export control obligations and nonproliferation consequences. See the [PNNL Counterintelligence](#) web page for more information.

For more information about PNNL's supply chain security, see the [Center for Global Security](#) web page. For guidance on what information should be reviewed prior to external release, contact the [Information Release SME](#) or [Export Control](#) team. Also, in HDI, review the [Information Release](#) page, and see the [Deliver Information Product](#) work control.

If you have questions about this article or have a lesson to share, please contact the Operating Experience / Lessons Learned Program Manager, [Patti Ammonet](#) at 375-2275.

## Related Articles

 	<a href="#">Video: Sensitive Nuclear Technology</a>	Security	11/12/2013
 	<a href="#">Chains Used in CM Hoists Could Lead to Failure after Extended Use</a>	Quality	5/27/2009
 	<a href="#">Holiday Reminders - Be Security Smart</a>	Security	10/27/2011
 	<a href="#">Video: Release of technology</a>	Security	11/13/2013

## Comments

Add Your Comment:

1000 characters left

Add

## Article Comments

[Subscribe to comments on this article.](#)

No readers have yet commented.

Add comment

Lessons Contacts: [Patti Ammonet](#) 375-2275 | [Penny Gouge](#) 375-2788 | [Shannon Cartier](#) 375-4316



**Pacific Northwest**  
NATIONAL LABORATORY

*Proudly Operated by **Battelle** Since 1965*

902 Battelle Boulevard  
P.O. Box 999  
Richland, WA 99352  
1-888-375-PNNL (7665)

U.S. DEPARTMENT OF  
**ENERGY**

---

[www.pnnl.gov](http://www.pnnl.gov)