# FINAL WORKSHOP REPORT

# GLOBAL SUPPLY CHAIN SECURITY STANDARDS

A PUBLICATION OF THE
ANSI HOMELAND SECURITY STANDARDS PANEL

NOVEMBER 2012

ANSI
American National Standards Institute

# Workshop Report

**Global Supply Chain Security Standards**

Report prepared November 2012

## 1.0 Background

In January 2012, the White House released a *National Strategy for Global Supply Chain Security*[1] to protect the nation's reliance upon the worldwide network of transportation, postal, and shipping assets and supporting infrastructures that make our dynamic trade system possible.
Since 2003, the American National Standards Institute (ANSI) Homeland Security Standards Panel (HSSP)[2] has worked to accelerate the development of voluntary standards for homeland security and emergency preparedness in support of the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T).

As part of that continuing effort, ANSI-HSSP hosted a workshop on September 12-13, 2012, to provide an overview of the national strategy and the status of the related standardization work being done in the public and private sectors. The event also served as the ANSI-HSSP plenary meeting for 2012.

## 2.0 Workshop Structure

The workshop opened with introductory remarks providing an overview of the national strategy and its development, and emphasizing the continuing need for standards in this area.

This introduction was followed by a panel discussion exploring current implementation efforts related to the national strategy. The next panel described current international programs aimed at protecting the global supply chain. A third panel provided an overview of current U.S. federal programs aimed at protecting the supply chain. The final panel of day one focused on current private-sector supply chain security programs.

Day two of the workshop began with a panel on current anti-counterfeiting efforts in the global supply chain. The second panel of the day provided an overview of current standards supporting anti-counterfeiting measures. The third session served as the ANSI-HSSP plenary session, providing a background of the HSSP and a summary of recent HSSP activity. The workshop concluded with closing remarks by the workshop co-chairs.

[1] http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf
[2] http://www.ansi.org/hssp

## 3.0 Welcome and Opening Remarks

Fran Schrotter, ANSI senior vice president and chief operating officer, opened the meeting and expressed her appreciation to the workshop co-chairs, Phil Mattson and his team at DHS, and Dr. Bert Coursey of the National Institute of Standards and Technology (NIST), for all of their efforts and leadership in putting the workshop together.

Ms. Schrotter provided background on ANSI and noted that the HSSP is an example of standards coordination through a public-private partnership to address the nation's needs.

Ms. Schrotter noted that we must examine the security measures that will ensure quality and safety in the supply chain for U.S. consumers. She added that a strong partnership between the public and private sectors is critical to addressing this national and global priority.

Next, Christa Brzozowski, White House national security staff, began her remarks by describing the *National Strategy for Supply Chain Security* as a high-level document that is not only a security strategy but also provides insight on protecting and strengthening the global supply chain system through a common unified vision.

Ms. Brzozowski identified two goals of the strategy: promoting the global supply chain and making sure it is secure and efficient, and enhancing the resilience of the system. She added that the strategy examines the global supply chain in a non-regulatory way, and clarified that the document is not industry specific as its scope includes air, land, sea, exports, and imports. Ms. Brzozowski emphasized that collaboration is needed between the private sector and all levels of government in order for the strategy to be successful.

**Goals of the National Strategy:**

✓ Promote the global supply chain, ensuring security and efficiency

✓ Enhance overall resilience of the system

Ms. Brzozowski noted that, through a seven-month process, DHS will consolidate input on the strategy and provide recommendations. She added that the harmonization of requirements and policies for public-private partnerships, and a shift away from command and control towards mutual recognition and trusted industry partners, are some of the results the administration hopes to achieve through the review process. Ms. Brzozowski concluded her remarks by emphasizing the need for collaboration between the public and private sectors in order to make the strategy successful.

**Some areas for improvement:**

✓ Harmonize requirements and policies

✓ Shift away from "command and control" by government towards mutual recognition and industry partnerships

## 4.0 Panel Discussion: White House Global Supply Chain Security Strategy Implementation Plan

Sean Moon, acting director, transportation and cargo, DHS Office of Transborder Policy, provided an overview of the implantation efforts of the national strategy. Mr. Moon described the strategy as aiming to foster a more resilient system that can prepare and withstand evolving threats and interruptions. He further noted that the strategy is only the beginning of a process that will result in federal implementation plans.

Mr. Moon stated that interagency and national security staff has identified several goals to be accomplished in the first year following approval of the strategy, and that multiple working groups are being formed to target these actions. As one example, he noted that the information sharing working group would look to enhance government-wide utilization of data and determine how to harmonize that data with the private sector.

All government strategies should be reviewed with a focus on supply chain

He described the national strategy as a keystone document that impacts multiple other strategies across the federal government. Mr. Moon added that all government strategies need to be reviewed with a focus on supply chain in order to ensure that there is a clear, non-conflicting message.

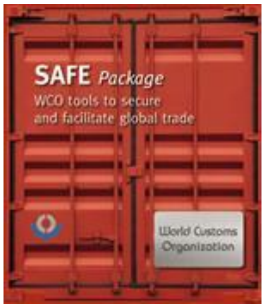
Mr. Moon highlighted the search for standards that were applicable to the global supply chain and identified six treaty organizations, four international standards developing organizations, five regional trade organizations, and seven private-sector organizations that currently have standards in this area. Mr. Moon noted that only 1% of the existing standards support the national strategy. He stated that standards are needed that are specific enough to be real and measurable but flexible enough to be applied in different areas. Mr. Moon concluded his remarks by urging the attendees to focus on how to expand the large gaps in standards in order to create an efficient global supply chain security system.

## 5.0 Panel Discussion: International Policy and Perspective

Panelists included:

- Dominique Tarpey, DHS Transportation Security Administration (TSA)
- Leticia Pibida, NIST; International Electrotechnical Commission (IEC) Subcommittee (SC) 45
- Simon Royals, Senior Technical Officer, Facilitation & Procedures Sub-Directortate, World Customs Organization (WCO)
- Paolo Salieri, Principal Scientific/Policy Officer, European Commission, DG Enterprise and Industry Security Research & Development
- Lilian Bertin, Principal Administrator, European Commission

**SAFE Framework of Standards**


SAFE Package
WCO tools to secure and facilitate global trade
World Customs Organization

The SAFE Framework of Standards aims to secure and facilitate global trade through supply chain security and facilitation standards. The World Customs Organization (WCO) Council adopted the SAFE Framework in 2005.

**European Union and U.S. Common Approach**

The U.S. and the European Union (EU) share a common approach to supply chain security. The global supply chain security policy should be risk based and cost effective, and should facilitate secure transport operations. Both the United States and the EU recognize the need to improve interagency and international coordination as supply chain security is a cross cutting issue which concerns several sectors (law enforcement, customs, etc.).

A mutual recognition agreement between the U.S. and EU was reached in May 2012 for trade publishing programs, and in June 2012 a mutual recognition agreement between the U.S. and EU was announced for air cargo security regimes. There is currently an effort to have mutual recognition on security controls at seaports. It is important for guidelines to be established for mutual recognition agreements so that everyone is operating the same way.

**Standards vs. Guidelines**

Broad global guidelines are complimentary to technical standards. Guidelines are more flexible and may allow for a variety of implementation methods, where technical standards are specific. Flexible guidelines may be useful in helping to harmonize existing standards.

**Standards Development and Cost**

Consensus standards and government standards are developed for global supply chain security based on need. Standards developers should constantly survey the global supply chain arena in order to determine the need for future standards and testing. That said, the cost of both standards and testing may be a deterrent for some organizations. There is a strong need for end-user incentives to adopt the standards and tests.

## 6.0 Panel Discussion: U.S. Federal Programs and Perspectives

Panelists included:

- Shawn Beddows, Program Manager C-TPAT, Customs and Border Protection Trusted Shipper Programs, DHS
- Mike Kangior, Director, Resilience Policy, DHS Policy Office
- Brett Laduzinsky, Risk Characterization Group, U.S. Customs and Border Protection (CBP)
- David Taylor, Program Manager, DHS S&T, Technology needs for Global Supply Chain Security
- Captain Drew Tucci, U.S. Coast Guard

**Resilience STAR**

The DHS Resilience STAR Program is a voluntary certification initiative targeting 18 specific sectors. The first sectors that will take part in the program will be the commercial facilities sector, which includes homes. Resilience standards for water, cybersecurity, and transportation are also being examined as part of the program.

**Risk Characterization**

The DHS working group on risk characterization is already moving forward with one of the national strategy goals: better identifying and assessing risk within the supply chain. As a first step, the working group has examined existing studies and assessments with the goal of creating a flexible framework that could evolve as more information is gathered. The group has already determined the need for harmonization of metrics, terminology, and standards that are used by the government and the private sector.

**U.S.-EU Supply Chain Security Pilot**

A joint U.S. – EU Supply Chain Security Pilot is in the planning stage. It will test and evaluate next generation cargo security technologies and share lessons learned on technology performance. In addition, it will exchange real-time tracking data and demonstrate data security via data encryption.

**Maritime Transportation Security Act (MTSA)**

The *Maritime Transportation Security Act* was developed shortly after the events of 9/11. The MTSA was passed by Congress in order to implement the International Ship and Port Facility Security Code (ISPS) in the United States. The MTSA requires DHS to learn more about the anti-terrorism measures in foreign ports.

According to Rep. Frank A. LoBiondo, chairman of the Coast Guard and Maritime Transportation Subcommittee, “MTSA was a landmark piece of legislation that established a framework to improve the security of the nation’s ports, waterways, and vessels from potential terrorist attacks.”

> “The importance of keeping our ports and waterways secure cannot be overstated. Approximately 90 percent of all global trade and over 25 percent of our Gross Domestic Product moves via the sea. A terrorist attack at our ports could severely disrupt the supply chain, which would be catastrophic to our fragile economy.”
> – Rep. Frank A. LoBiondo

## 7.0 Panel Discussion: Private-Sector Programs and Perspectives

Panelists included:

- Gordon Gillerman, Director, Standards Services Group, NIST
- Mark Miller, Founder, President, and CEO, CONCEPTIVITY S.à.r.l.; European Organisation for Security (EOS) Vice Chairman; EOS Board of Directors Chairman; EOS Supply Chain Security Working Group

- Bernie Hogan,GS-1, Senior Vice-President, Emerging Capabilities & Industries
- David A. Brown, Senior Principal Engineer, Product Fraud Countermeasures, Intel Corporation
- Corey C. Jones, Security & Fire Protection, Supply Chain & Aviation Security Compliance, The Boeing Company
- David Wilt, Global Supply Chain Security Manager, Xerox Corporation

**Standards Collaboration**

Voluntary consensus standards are developed in a collaborative process by a balanced group of stakeholders. The collaborative spirit of standards development should be applied to, first, increase the commonalities between similar standards, and second, ensure that conformity assessment requirements are harmonized. An ideal situation would be a system of global supply chain standardization that relies upon a single conformity assessment solution.

**C-TPAT**

The Customs-Trade Partnership against Terrorism (C-TPAT) is a voluntary initiative that builds cooperative relationships to strengthen and improve the international supply chain and U.S. border security. Organizations that are part of the C-TPAT program use a risk-based approach to ensure that the C-TPAT criteria are embedded in contracts with vendors and suppliers. Participants are motivated to comply with the requirements, since the loss of C-TPAT certification impacts business revenue as well as security issues in the supply chain.

**Assessment Methods**

Some organizations have found that third-party assessment is too costly and have chosen to do their own assessment of conformity. The cost of third-party assessment is mitigated by some organizations using internal assessment tools. But in some sectors, such as air cargo, third-part assessment has been a successful solution when the government cannot cover all aspects of the assessment review.

## 8.0 Panel Discussion: Anti-Counterfeiting in the Supply Chain

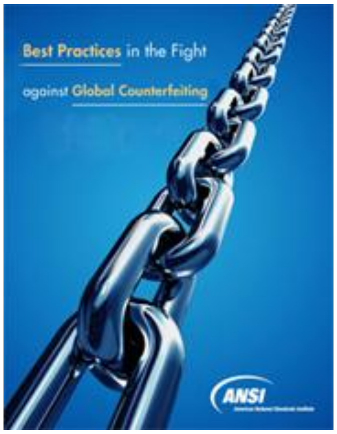
Panelists included:

- Michael O'Neil, Executive Director, North American Security Products Organization (NASPO)
- Don Davidson, Chief Outreach, Science & Standards for CNCI-SCRM, Trusted Mission Systems and Networks, U.S. Department of Defense (DOD)
- Jon Amis, Program Director, Supply Chain Assurance, Dell, Global Supply Chain
- Juan Marcos Baez, Corporate Security Director, Bristol Myers Squibb
- David A. Brown, Senior Principal Engineer, Product Fraud Countermeasures, Intel Corporation
- Ron Guido, Vice President, Global Brand Protection and Supply Chain Integrity, Johnson & Johnson

### Scope of the Problem

Counterfeiting is a growing global concern that crosses all borders and victimizes government, businesses, and consumers alike. Estimates put the economic cost to U.S. companies alone at $250 billion, and annual American job loss at 750,000. Safety risks, health issues, and the operation of dangerous criminal enterprises make counterfeiting even more damaging to people around the world.

In an effort to identify and communicate cross-sector solutions to this global challenge, ANSI has published a free report, *Best Practices in the Fight against Global Counterfeiting: An Action Guide to Strengthen Cooperation and Collaboration across Industry Sectors and among Global Supply Chains*. [3]



### Standards Needs

Anti-counterfeiting efforts must be based on a risk-based strategy. Industry standards currently being developed for supply chain security must also be applied to the anti-counterfeiting arena. There is a need for standards to be developed that are effective for both new and old technologies. Standards must also encompass both individual parts and entire systems. One key challenge identified in the development of new standards is applicability across various industries.

### Supplier Selection

A defined supplier selection process will help protect against counterfeiting by ensuring that only approved suppliers develop and manufacture products. It is important to verify the supplier's capability to manage and control their supply chain partners. In addition, suppliers must maintain a chain of custody for all products, parts, and systems.

### Information Sharing and Collaboration

Best practices need to be shared within industry to combat counterfeiting. There is no competitive advantage to be gained by withholding an organization's anti-counterfeiting plan. Information sharing and collaboration within industry would help to develop universal competency in supply chain integrity. Law enforcement is an effective deterrent; however, consumer awareness and more advanced detection technologies can also help reduce or prevent the counterfeiting problem.

[3] http://publicaa.ansi.org/sites/apdl/Documents/Meetings%20and%20Events/2010%20World%20Standards%20Week/Anti-counterfeiting%20Conference/Anti-Counterfeiting_Best_Practices.pdf

## 9.0 Panel Discussion: Standards for Anti-Counterfeiting in the Global Supply Chain

Panelists included:

- Gordon Gillerman, Director, Standards Services Group, NIST
- Randy Dougherty, Vice President, ANSI-ASQ American National Accreditation Board (ANAB)
- Mary G. Foster, PharmD, Corporate Vice President Quality and Regulatory Affairs, Aphena Pharma Solutions, U.S. Pharmacopeial
- Joe Lewelling, Vice-President of Standards Development, Association for the Advancement of Medical Instrumentation (AAMI)
- Bruce Mahone, Director, SAE International
- Michael O'Neil, Executive Director, NASPO

**Requirements for an Organization Conducting Conformity Assessment**
The role of the conformity assessment body is to determine if an organization has effectively implemented a standard. In order to do so, the conformity assessment body must be impartial and demonstrate its competence at certifying organizations. Since the implementation of standards by industry is a key aspect of anti-counterfeiting, assessing conformance to those standards is of critical importance to supply chain integrity.

**ISO Technical Committee 247**
International Organization for Standardization (ISO) Technical Committee (TC) 247, *Fraud Countermeasures and Controls*, focuses on standardization in the field of detection, prevention, and control of fraud. Counterfeiting and identity theft are included in the scope of work of TC 247, and any area under counterfeiting can be added to the scope of the broad work of TC 247 as needed. TC 247 works to create international standards relating to fraud in areas including supply chains for security technologies, products, and/or material goods of value and service components.

**Role of Standards**
Standards can create a global infrastructure that will assist in identifying and reporting counterfeits.

Standards can provide guidance and consistency, and they can unify organizations against counterfeiting.

Standards for manufacturers and importers can help to stop counterfeiting.

But standards can only do all of these things when they are consistently adopted by organizations. Risk assessment standards need to be applied to the full supply chain, including areas that are not addressed in existing standards such as distributers and purchasers.

## 10.0 HSSP Plenary

The HSSP Plenary session was presented by ANSI-HSSP public sector co-chair Gordon Gillerman, Director, Standards Services Group, NIST. Mr. Gillerman provided a background on the ANSI-HSSP, noting that the HSSP is based on a public-private partnership.

Mr. Gillerman noted that standards are a natural place for collaboration in order to provide security solutions. He added that those solutions will not come from a single stakeholder but from the community at large by consensus development, making the ANSI-HSSP an ideal place to collaborate on standards needs in the homeland security arena.

Mr. Gillerman described the White House strategy as highlighting the importance of the ANSI-HSSP, since much of the work that needs to be done in supply chain security will be done in the private sector. Mr. Gillerman added that supply chain security and other areas of homeland security–related concern require a framework of standards, and that the ANSI-HSSP can learn from the success of standards coordination activities in other sectors.

## 11.0 Closing Remarks/Adjournment

The workshop co-chairs, Sean Moon and Michael O'Neil, provided the closing remarks. They stated that the core of global supply chain security is trust and confidence in what is being manufactured and moved. Mr. Moon added that commercially acceptable global standards must be derived from industry best practices using a collaborative approach, as all industry is responsible for securing the global supply chain. Mr. O'Neil added that he hoped the work discussed at this workshop will continue in the future.

## Appendix 1 Agenda

ANSI Homeland Security
Standards Panel (ANSI-HSSP)

**Workshop Co-Chairs:**

- **Sean K. Moon, Director (Acting), Transportation and Cargo, Office of Transborder Policy, U.S. Department of Homeland Security**
- **Michael O'Neil, Executive Director, North American Security Products Organization (NASPO)**

A Workshop on:

**Global Supply Chain Security Standards and Annual Plenary Meeting**

**Final Agenda**

**Wednesday, September 12, 2012 – Thursday, September 13, 2012**

**Location:**
The FHI 360 Conference Center
1825 Connecticut Avenue, NW
8th Floor (Academy Hall)
Washington, DC 20009-5721

| **DAY 1 – Wednesday, September 12, 2012** | |
|---|---|
| 8:30am – 9:00am | **Registration Desk Opens** |
| 9:00am – 9:45am | **Welcome & Opening Remarks**<br>• Frances E. Schrotter, Senior Vice-President and Chief Operating Officer, American National Standards Institute (ANSI)<br>**U.S. National Strategy on Global Supply Chain Security**<br>**Keynote Speaker:**<br>• Christa Brzozowski, White House, National Security Staff<br>*The focus of the National Strategy is the worldwide network of transportation, postal, and shipping pathways, assets, and infrastructures by which goods are moved from the point of manufacture until they reach an end consumer, as well as supporting communications infrastructure and systems. Ms. Brzozowski will provide an overview of the national strategy and its development.* |
| 9:45am - 10:00am | **White House Global Supply Chain Security Strategy Implementation Plan**<br>*Embracing the President's commitment to collaboration with global supply chain stakeholders, following the release of the Strategy, the government began implementation through a series of working groups, including groups focused on global standards and domestic and international outreach to other governments and the private sector. Mr. Moon will provide an overview of the implementation efforts and initial insights into some of the stakeholder input received.*<br>**Presenter:**<br>• Sean K. Moon, Director (Acting), Transportation and Cargo, Office of Transborder Policy, U.S. Department of Homeland Security (DHS) |

| | |
|---|---|
| 10:00am - 11:00am | **International Policy and Perspective**<br>*There are international and regional efforts to protect the global supply chain. The panelists will provide an overview of their programs as well as their recent activities.*<br><br>**Presenters:**<br>• Dominique Tarpey, U.S. Department of Homeland Security (DHS), Transportation Security Administration (TSA)<br>• Leticia Pibida, National Institute of Standards & Technology (NIST), *IEC SC 45*<br>• Simon Royals, Senior Technical Officer, Facilitation & Procedures Sub-Directortate, World Customs Organization (WCO)<br>• Paolo Salieri, Principal Scientific/Policy Officer, European Commission, DG Enterprise and Industry Security Research & Development<br>• Lilian Bertin, Principal Administrator, European Commission<br><br>**Audience Q&A** |
| 11:00am - 11:15am | **Morning Break** |
| 11:15am - 12:30pm | **International Policy and Perspectives (Continued from the Morning)** |
| 12:30pm – 1:30pm | **Lunch** |
| 1:30pm - 3:00pm | **U.S. Federal Programs and Perspectives**<br><br>**Presenters:**<br>• Shawn Beddows, Program Manager C-TPAT, Customs and Border Protection Trusted Shipper Programs at Department of Homeland Security (DHS)<br>• Mike Kangior, Director, Resilience Policy, U.S. Department of Homeland Security (DHS) Policy Office<br>• Brett Laduzinsky, Risk Characterization Group, CBP<br>• David Taylor, Program Manager, U.S. Department of Homeland Security (DHS) Science & Technology Directorate, Technology needs for Global Supply Chain Security<br>• Captain Drew Tucci, U.S. Coast Guard<br><br>**Audience Q&A** |
| 3:00pm - 3:15pm | **Afternoon Break** |
| 3:15pm - 4:45pm | **Private Sector Programs and Perspectives**<br><br>**Moderator:** Gordon Gillerman, Director, Standards Services Group,<br>National Institute of Standards and Technology (NIST)<br><br>**Presenters:**<br>• Mark Miller, Founder - President and CEO CONCEPTIVITY S.à.r.l. , European Organisation for Security (EOS) Vice Chairman, EOS Board of Directors Chairman, EOS Supply Chain Security Working Group<br>• Bernie Hogan,GS-1, Senior Vice-President, Emerging Capabilities & Industries<br>• David A. Brown, Senior Principal Engineer, Product Fraud Countermeasures, Intel Corporation |

| | |
|---|---|
| | • Corey C. Jones, Security & Fire Protection, Supply Chain & Aviation Security Compliance, The Boeing Company<br>• David Wilt, Global Supply Chain Security Manager, Xerox Corporation<br><br>**Audience Q&A** |
| 4:45pm - 5:30pm | **Closing Remarks/Adjournment**<br>• Sean K. Moon, Director (Acting), Transportation and Cargo, Office of Transborder Policy, U.S. Department of Homeland Security (DHS)<br>• Michael O'Neil, Executive Director, North American Security Products Organization (NASPO) |
| 5:30pm - 7:00pm | **Networking Cocktail Reception**<br>Darlington House<br>1610 20th Street NW<br>Washington, DC 20009<br><br>Note: International participants to the ISO Special Advisory Group – Security (ISO SAG-S) being held on September 13-14, are invited to the reception for networking as well. |
| **DAY 2 - Thursday, September 13, 2012** | |
| 8:30am – 9:00am | **Registration Desk Opens** |
| 9:00am – 9:10am | **Opening Remarks** |
| 9:10am – 11:00am | **Anti-Counterfeiting in the Supply Chain**<br>*The panelists will provide a short presentation on their organizations anti-counterfeiting efforts in the global supply chain. The moderator will then lead a roundtable discussion with the panelists and the audience.*<br><br>**Moderator:** Michael O'Neil, Executive Director, North American Security Products Organization (NASPO)<br><br>**Panelists:**<br>• Don Davidson, Chief Outreach, Science & Standards for CNCI-SCRM, Trusted Mission Systems & Networks, U.S. Department of Defense<br>• James Stein, Government-Industry Data Exchange Program (GIDEP) Program Manager Defense Standardization Program Office, Office of the Assistant Secretary of Defense (Research and Engineering/Systems Engineering), Department of Defense<br>• Jon Amis, Program Director, Supply Chain Assurance, Dell, Global Supply Chain<br>• Juan Marcos Baez, Corporate Security Director, Bristol Myers Squibb<br>• David A. Brown, Senior Principal Engineer, Product Fraud Countermeasures, Intel Corporation<br>• Ron Guido, Vice President, Global Brand Protection & Supply Chain Integrity, Johnson & Johnson |
| 11:00am – 11:15am | **Morning Break** |

| | |
|---|---|
| 11:15am – 12:15pm | **Standards for Anti-Counterfeiting in the Global Supply Chain**<br>*There are International and National efforts in anti-counterfeiting. The panelists will provide an overview of their standards as well as their recent activities.*<br>**Introduction:** Gordon Gillerman, Director, Standards Services Group,<br>National Institute of Standards and Technology (NIST)<br>**Standards & Conformity Assessment Program Presenters:**<br>• Randy Dougherty, Vice President, ANSI-ASQ American National Accreditation Board (ANAB)<br>• Mary G. Foster, PharmD, Corporate Vice President Quality & Regulatory Affairs, Aphena Pharma Solutions, U.S. Pharmacopeial<br>• Joe Lewelling, Vice-President of Standards Development, Association for the Advancement of Medical Instrumentation ( AAMI)<br>• Bruce Mahone, Director, SAE International<br>• Michael O'Neil, Executive Director, North American Security Products Organization (NASPO)<br>**Audience Q&A** |
| 12:15pm – 12:45pm | **HSSP Plenary**<br>*A summary of the workshop will be presented. The audience will be encouraged to participate in the dialogue on what the next steps for HSSP and which upcoming initiatives that should be supported.*<br>**ANSI-HSSP Co-Chair:**<br>• Gordon Gillerman, Director, Standards Services Group,<br>National Institute of Standards and Technology (NIST) |
| 12:45pm – 1:00pm | **Closing Remarks/Adjournment**<br>**Workshop Co-Chairs:**<br>• Sean K. Moon, Director (Acting), Transportation and Cargo, Office of Transborder Policy, U.S. Department of Homeland Security<br>• Michael O'Neil, Executive Director, North American Security Products Organization (NASPO) |

## Appendix 2 Roster of Attendees

| First Name | Last Name | Organization |
|---|---|---|
| Daniel | Ackerman | U.S. Department of Homeland Security (DHS) |
| Jon | Amis | Dell |
| Joseph | Andersen | Telecommunications Industry Association |
| Shawn | Beddows | U.S. Department of Homeland Security (DHS) |
| Gisele | Bennett | Georgia Tech |
| Lilian | Bertin | European Commission |
| Elizabeth | Board | GS1 |
| Jon | Boyens | National Institute of Standards and Technology (NIST) |
| David | Brown | Intel |
| Christa | Brzozowski | White House |
| Stephen | Caldwell | GAO |
| Jessica | Carl | American National Standards Institute (ANSI) |
| Donggeun | Choi | National Institute for Standards and Technology (NIST) |
| Scott | Cooper | American National Standards Institute (ANSI) |
| Bert | Coursey | National Institute of Standards and Technology (NIST) |
| Michael | Cox Jr. | U.S. Department of Homeland Security (DHS) |
| Henry | Cuschieri | International Organization for Standardization (ISO) |
| Don | Davidson | U.S. Department of Defense |
| Michelle | Deane | American National Standards Institute (ANSI) |
| Lori | Denham | Kountoupes Consulting LLC |
| Randy | Dougherty | ANSI-ASQ American National Accreditation Board (ANAB) |
| Marianne | Elbertson | USDA-FSIS |
| Manabu | Eto | Japanese National Committee for SAG-S |
| Mary | Foster | Aphena Pharma Solutions |
| Gordon | Gillerman | National Institute of Standards and Technology (NIST) |
| Karlhanns | Gindele | DIN |
| Ron | Guido | Johnson & Johnson |
| Ed | Harrison | Cargo Intelligence Security and Logistics Association |
| Paul | Hobart | U.S. Government Accountability Office (GAO) |
| Bernie | Hogan | GS-1 U.S. |
| Jeffrey | Horlick | National Institute of Standards and Technology (NIST) |
| Ajit | Jillavenkatesa | National Institute of Standards and Technology (NIST) |
| Corey | Jones | The Boeing Company |

| First Name | Last Name | Organization |
|---|---|---|
| Ryan | Kane | U.S. Department of Commerce |
| Mike | Kangior | U.S. Department of Homeland Security (DHS) |
| Donald | Kautter | U.S. Department of Agriculture |
| Robert | Knetl | Georgia Tech Research Institute |
| John | Kulick | Siemens USA |
| Brett | Laduzinsky | CBP |
| Helen | Lawrence | FBI |
| Joe | Lewelling | AAMI |
| Igor | Linkov | U.S. Army Engineer Research and Development Center |
| Henrik | Madsen | IMO Maritime Security Section |
| Bruce | Mahone | SAE International |
| Juan | Marcos Baez | Bristol Myers Squibb |
| Toshihiro | Matsui | Japanese National Committee for SAG-S |
| Phil | Mattson | U.S. Department of Homeland Security (DHS) |
| Elizabeth | McDaniel | IDA |
| Jonathan | McEntee | U.S. Department of Homeland Security (DHS) |
| Tim | McGarr | BSI Group |
| Mark | Miller | Conceptivity |
| Warren | Miller | Transportation Security Administration |
| Sean | Moon | U.S. Department of Homeland Security (DHS) |
| David | Moreno | Federal Bureau of Investigation |
| Marie | Myint | Transportation Security Administration |
| Ichiro | Nakajima | Japanese National Committee for SAG-S |
| Kevin | O'Brien | Revere |
| Michael | O'Neil | North American Security Products Organization (NASPO) |
| Celie | Paulson | National Institute of Standards and Technology (NIST) |
| Leticia | Pibida | National Institute of Standards and Technology (NIST) |
| Marcus | Pollock | U.S. Department of Homeland Security (DHS) |
| Erik | Puskar | National Institute of Standards and Technology (NIST) |
| Ed | Rao | U.S. Department of Homeland Security (DHS) |
| Karen | Reczek | National Institute of Standards and Technology (NIST) |
| Paul | Ross | Dynamic Security Concepts, Inc. |
| Simon | Royals | World Customs Organization (WCO) |
| Paolo | Salieri | European Commission |
| Amy | Sanborn | U.S. Department of Homeland Security (DHS) |

| First Name | Last Name | Organization |
|---|---|---|
| Paul | Schomburg | Panasonic Corporation of North America |
| Fran | Schrotter | American National Standards Institute (ANSI) |
| Fred | Schwien | The Boeing Company |
| Peter | Shebell | U.S. Department of Homeland Security (DHS) |
| Maranda | Sorrells | U.S. Department of Homeland Security (DHS) |
| James | Stein | U.S. Department of Defense |
| Julie | Szegda | U.S. Department of Homeland Security (DHS) |
| Dominique | Tarpey | U.S. Department of Homeland Security (DHS) |
| David | Taylor | U.S. Department of Homeland Security (DHS) |
| Drew | Tucci | U.S. Coast Guard |
| Tracy | Wilson | Pacific Northwest National Laboratory |
| David | Wilt | Xerox Corporation |
| Nohemi | Zerbi | U.S. Department of Homeland Security (DHS) |