NISTIR 7861

The Benefits of U.S.-European Security Standardization

http://dx.doi.org/10.6028/NIST.IR.7861

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 7861

The Benefits of U.S.-European Security Standardization

Erik Puskar
Standards Coordination Office
Laboratory Programs

http://dx.doi.org/10.6028/NIST.IR.7861

June 2012

U.S. Department of Commerce
John E. Bryson, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

Acknowledgements

The Standards Coordination Office of NIST and the Joint Research Centre (JRC) of the European Commission prepared this document jointly. Those contributing include: Gianmarco Baldini, Klaus Keus, Alois J. Sieber, and Goeran Loevestam from JRC; Christoph Kautz, European Commission DG ENTR; and Bert Coursey, Gordon Gillerman, David Leech (consultant), and Erik Puskar of NIST. Also providing support to this effort were Robert Zimmerman and Yonas Nebiyeloul-kifle of the Homeland Security Institute.

Disclaimer

The opinions expressed by the European contributors are those of the author(s) only and should not be considered as representative of the European Commission's official position.

Table of Contents

List of Figures

List of Tables

1. Purpose

The goal of this concept paper is to articulate the rationale for why further European-U.S. collaboration on security standardization *should* be undertaken.

In April 2010, the European Commission's Joint Research Centre (JRC) initiated a process of U.S.-EU collaboration on security standards. In November 2010, American National Standards Institute (ANSI) hosted the Ninth Plenary Session of the HSSP (Homeland Security Standards Panel): U.S.-European Collaboration on Security Standardization Systems. A keynote presentation, by Rolf Dietrich (Deputy under Secretary for Science and Technology (Acting), U.S. Department of Homeland Security), called for a broad agenda of U.S.-European Union (EU) collaboration, including:

- Coordinating with partner nations to identify viable areas for cooperation and partnering
- Developing strategic priorities with other Federal agencies in support of the homeland security mission
- Matching U.S. entities engaged in homeland security research with foreign counterparts so that they may partner in cooperative research activities
- Engaging international partners to participate in the DHS Centers of Excellence program and encouraging U.S. institutions to partner with academic institutions abroad
- Requiring grant recipients to include both U.S. and foreign institutions
- Cooperating with partner nations on development and implementation of standards for key areas such as border security and supply chain security.[1]

The outcome of the ANSI-HSSP session was a pledge to identify the gaps in, and priorities for, EU-U.S. collaboration; to foster the collaboration with the EU through European Standards Organizations by further dialogue on homeland security standardization; and to articulate the benefit of international standardization on cross-border issues.[2]

This paper sets out to develop the case for why these initiatives *should* be undertaken and identifies some possible high-yield areas for consideration. This argument will help the proponents sustain their efforts in the face of other pressing demands.

2. Introduction

There are many reasons — political, operational, and economic — why the European Union (EU) and the United States (U.S.) should cooperate in the development of security standards. There are many indicators of high levels of commitment to greater EU-U.S. security strategy

1. Rolf Dietrich, *U.S. – European Collaboration on Security Standardization Systems*, November 9-10, 2010.
2. *Ninth ANSI-HSSP Plenary: U.S. European Collaboration on Security Standardization Systems*, Open Discussion, Moderated by Gordon Gillerman, National Institute of Standards and Technology, November 10, 2010

integration.[3] This paper is consistent with such a commitment and offers a baseline for further discussions and concrete actions. It briefly characterizes the benefits of collaboration, focusing on the innovations and efficiencies that standardization entails. U.S.-EU standards institutions and collaborative standardization initiatives are identified; the logic of expanding EU-U.S. security standardization is developed and the process of the ensuing economic value creation is described. Thoughts on how security standards collaboration will work are provided and potentially fruitful areas of cooperation are suggested.

Standards are enablers of collaboration. The development of national and international security standards translates into enhanced security and accelerated introduction of innovative and cost-saving solutions for security mission needs. At the highest level, the anticipated benefits of greater EU-U.S. collaboration are the following:

- **Enhanced security measures** —Both the U.S. and EU promote a multi-layered strategy to combat terrorism and enhance security.[4] The multinational nature of the terrorist threat and the well-established interdependence of the EU and U.S. make cooperation critical. In fact, the 2002 National Strategy for Homeland Security acknowledged that "a successful strategy for homeland security requires international cooperation."[5] Integration and coordination of resources, assets and information are critical for ensuring the effectiveness of security measures. Standards provide the frameworks, lexicons and associated performance metrics necessary to coordinate, integrate and assess the performance of coordinated and integrated security measures. They provide the baseline by which all parties, including governments and international bodies could be held accountable for achieving desired security goals.

- **Innovation** — Standards can be tools for translating needs into capability requirements and scientific and technological specifications that drive product and process innovation across the security science and technology supply base. In the absence of standards, organizing fragmented security market segments and attracting innovative companies to work in this space becomes a daunting task. Innovators are forced to expend additional resources analyzing needs and articulating the capability requirements of security entities. In addition they are often forced to invest in test and evaluation (TandE) protocols to objectively evaluate or prove their solutions' superiority. Without input from an expert community such as provided in a standards development environment, the validity of test methods can be open to question. If innovative companies cannot achieve an economic premium for their innovations, then the economic incentive to innovate will be dampened or lost. Furthermore, *de-facto* standards developed and promulgated by large companies often create barriers of entry for smaller highly innovative companies.

- **Economic efficiencies** — In addition to fostering technical innovation, standards allow economic efficiencies to be achieved in the production and sale of existing security-related products and services. Standards benefit final consumers and product integrators

3. See *EU-U.S. Security Strategies: Comparative Scenarios and Recommendations* (The European Union Pilot Project on Transatlantic Methods for Handling Global Challenges in the European Union and United States), conducted jointly by the Istituto Affari Internazionali (IAI), the Swedish Institute of International Affairs (UI), the Fondation pour la Recherche Stratégique (FRS), and the Center for Strategic and International Studies (CSIS), 2011; and *EU-US Security and Justice Agenda in Action*, Patryk Pawlak (Editor), EU Institute for Security Studies, December 2011.
4. In the U.S. context, the multi-layered approach is referred to as "defense-in-depth."
5. U.S. Department of Homeland Security, *The National Strategy for Homeland Security*, 2002.

by reducing varieties and lowering the cost of acquiring product information ("search costs"), reducing transaction costs (by lowering qualification testing costs, acceptance testing costs and complaint and adjustment allowance costs) and lowering prices by providing a basis for more price and quality competition. Additionally, standards benefit suppliers by reducing market fragmentation, providing opportunities for economies of scale, enabling production process/quality control, by increasing the scope of interoperability and encouraging the optimization of product system designs.[6]

Both the U.S. and the EU are individually committed to a multi-layered strategy for enhancing homeland security and citizen protection composed of material and non-material solutions:

- **Outside borders —** The first layer involves closely coordinating diplomatic, military, and intelligence assets to find, track, and defeat terrorists abroad. This layer of the strategy is aimed at keeping foreign terrorists out, off balance, and on the run and to prevent their access to nuclear, chemical, biological, or radiological weapons of mass destruction.
- **At point of entry —** The second layer involves raising barriers at ports of entry. Key to this mission is real-time information sharing concerning the nationalities and whereabouts of known or suspected terrorists, and technologies for detecting explosives, weapons of mass destruction, etc., in airline baggage, freight, and shipping containers.
- **Within borders —** The third layer involves strengthening intergovernmental coordination/collaboration among federal, state, and local law enforcement agencies in order to detect, track, and defeat potential foreign and domestic terrorist activities within the borders. This third layer also involves building cooperation across the public and private sectors to protect the critical power, transportation, telecommunications, and other infrastructure that could represent targets for terrorists.

These individual elements add up to a set of strategies for layered security, starting from outside, through the intelligence and federal law enforcement networks guarding ports of entry, through the domestic law enforcement apparatus, down to the guards and concrete barriers on the perimeter of key facilities and the network administrators and others providing security inside them.

The location of security standards in the layered approach is illustrated in Figure 1. The security agencies are responsible for developing strategies to respond to the threats posed by attackers. At the general level, the strategy can be broken into four mission areas: prevention, protection, response, and recovery. Carrying out these missions in the most coordinated and cost effective manner requires standardization in all facets of the activities ("methods") required to implement the strategic mission areas.

6. Gregory Tassey, "Standardization of Technology-Based Markets," *Research Policy*, 29, 2000, pp. 587-602; and David Leech and John Scott, *The Economic Impacts of Documentary Standards: A Case Study of the Flat Panel Display Measurement Standard (FPDM)*, October 2011, especially Table 3-1, "Documentary Standards Economic Benefit Matrix," p. 18.

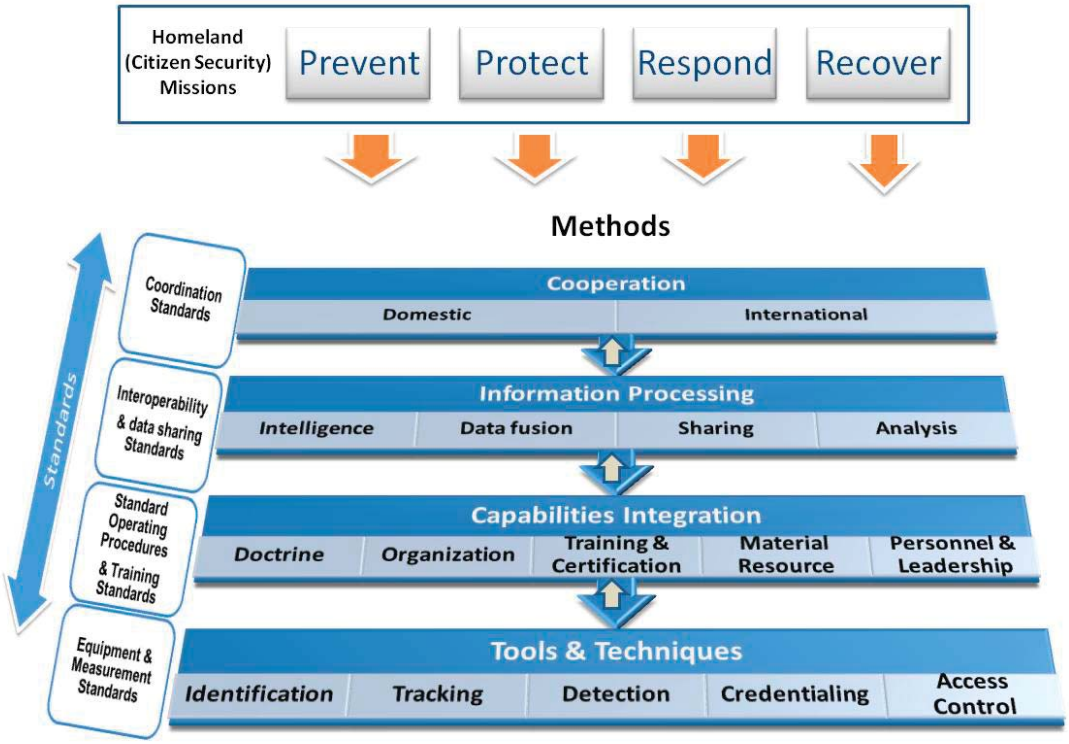

Figure 1. Homeland Security and Citizen Protection

Achieving progress toward defense-in-depth requires new ways of doing things (innovative products and services) and more cost effective ways of doing them (economic efficiencies). As depicted in Figure 1, these, in turn, are enabled by standardization efforts in support of coordination, interoperability, operating procedures, equipment acquisition and use, and training.

As the experiences of the U.S. show the involvement of standards developers early in the solution formulation stage of new technologies is crucial for accelerating innovation and encouraging the private sector's research and development (R&D) investments. Most importantly standards developers from government and industry proved invaluable in defining the operational requirements and setting performance metrics. They provided the technical platform for promoting exchange of technical and scientific information, and sharing of knowledge and best practices that channeled the efforts of innovative companies. For example, at the heart of aviation security is the ability to keep terrorists away from commercial airliners. Associated with this objective is the need to conduct passenger and cargo checkpoint screening at the point of origin. Technological solutions such as bulk explosive scanner systems used at checkpoints are evolving at a rapid pace due in part to the involvement of researchers knowledgeable in standardization at the front end of the needs identification and performance setting process. Without setting objective operational performance metrics early on, during the solution formulation stage, inconsistent performance would lead to lack of confidence requiring the application of additional screening measures. The added costs would have been either passed on to the taxpayer or the flying public. As discussed in the case study below, the security standardization process generates real benefits as well as economic value that accrues to

equipment manufacturers as well as buyers, both public and private which are passed along, ultimately, to consumers of safer transportation services.

From an economic perspective the use of internationally accepted standards spurs innovation, productivity, and economic growth; increases exports and imports; reduces barriers to market entry; induces network effects; reduces transaction costs; and increases trust between trading partners. Standards facilitate cross-border trade and give both buyers and sellers confidence in the quality, safety, and specification of goods that comply with those standards. They also reduce search costs that are particularly high for buyers of imported products and increase the potential for integrating the best research and technologies of the EU and the U.S.

The benefits of EU-U.S. security standards collaboration will depend on the positive changes caused by the new standards in terms of the resources devoted to the operations of security equipment manufacturers and equipment users; the resources devoted to ensuring that the volume and value of the transactions in goods and services are protected; and changes in the resources citizens devote to their security. While some of these benefits are very difficult to estimate, they are expected to derive from the following sources:

- Reduced requirements development costs for security equipment users
- Lower equipment costs or higher equipment quality due to increased competition
- Lower acquisition processing costs for security equipment users
- Decreased risk of failure and disruption for security equipment users (i.e., the failure of ineffective equipment and the subsequent costs of equipment recovery, repair, and re-installation)
- Increased speed with which standards are developed and adopted (nationally and internationally)
- Increased usefulness (process throughput or quality improvements) of new equipment relative to vintage (pre-standard) equipment
- Reduced qualification and certification costs, and thus reduced time-to-market
- Increased efficiency resulting from harmonized certification procedures at the international level
- Increased national market access for manufacturers
- Reduction in low-quality competitors
- Lower industry technology road mapping and product planning costs
- Increased EU-U.S. industry competitiveness from complying with external customer/market requirements
- Improved interoperability
- Removal of system integration barriers.

Through continued efforts by EU and U.S. proponents of security standards collaboration, a process has been launched to identify common priorities and specific areas for collaboration.

3. U.S. and European Institutions Supporting Homeland Security and Protection of the Citizen

Security Standard Setting in the U.S.

In the United States, the public-private sector partnership aimed at establishing standards for homeland security products and processes gained momentum in response to the terrorist attacks

of 2001. The Federal government established a new federal department, the Department of Homeland Security (DHS), by combining resources and aligning the missions of 22 different agencies from throughout the federal government. The initial organization in 2003 was organized along the lines of threats (chemical, biological, radiological/nuclear and explosives), borders and transportation security, emergency preparedness and response, and information analysis and infrastructure protection. Various private sector standards development organizations worked with the American National Standards Institute (ANSI) and U.S. federal agencies including the Office of Homeland Security, Department of Commerce/National Institute of Standards and Technology, Departments of Defense and Energy and the Environmental Protection Agency to form the Homeland Security Standards Panel (ANSI HSSP) in February 2003. Over the past decade DHS has reorganized the Department to better address the evolving threats to the nation. The present organization focuses on five broad areas: [7]

- Counterterrorism
- Border security
- Preparedness, response and recovery
- Immigration
- Cyber-security.

Within DHS, the Standards Branch of the Science and Technology Directorate coordinates standards activities. To gather standards requirements across the entire Department, they work with the DHS Standards Council, which is comprised of representatives from each of the sub-organizations that have important standards needs for meeting their mission requirements.

It is the policy of the Federal government to, where feasible, use standards developed by consensus in the private sector.[8] To be accepted, national standards must have credibility based on consensus. Thus, the DHS Office of Standards promotes the use of ANSI accredited, non-governmental standards development organizations (SDOs) to develop national standards for homeland security. The office invests in a wide spectrum of standards development projects to encourage and incentivize SDOs to develop standards for Homeland Security mission needs.

DHS has worked closely with the ANSI HSSP [www.ansi.org/standards] over the past eight years to convene workshops and conferences to address homeland security standards needs that cut across multiple standards development organizations. Key efforts to date include gathering standards requirements related to: private sector preparedness, biometrics, biological and chemical threat agents, training programs for first response to weapons of mass destruction (WMD) events, enterprise power security, perimeter security, lessons learned from Hurricane Katrina, emergency communications, financial sector risk and cyber-security, transit security standardization, emergency preparedness for persons with disabilities and special needs, and aviation security and resilience. An overview of each workshop is provided in the box below.

7. Each of these areas is covered in some detail on the DHS web site (www.dhs.gov).
8. The National Technology Transfer and Advancement Act (NTTAA), Public Law 104-113 (1995), directs federal U.S. agencies to use voluntary consensus standards, wherever possible, in lieu of creating proprietary, non-consensus standards.

American National Standards Institute – Homeland Security Standards Panel, Workshop and Report Summaries

The mission of the American National Standards Institute's Homeland Security Standards Panel (ANSI-HSSP) is to assist the U.S. Department of Homeland Security (DHS), and those sectors requesting assistance, in identifying, accelerating development of, and adopting consensus standards critical to homeland security. Brief summaries of HSSP workshops held since its inception follow. Date in heading refer to when report was released.

ANSI-HSSP Standards Related to Chemical Agents Workshop, December 2004

The ANSI-HSSP report on biochemical threats has a comprehensive breakdown of biological threats and potential biological indicators, identifying possible strategies for detection and other Homeland Security applications. The proposed outcome would be a report containing all known national and international standards and guidelines (published and under development), and any conformity assessment activities in the biological and chemical threat agents area.

ANSI-HSSP Biometric Standardization, April 2004

In order to identify areas for improvement and strategies to bring technologies forward, the ANSI-HSSP convened a Biometric Standardization Panel. Discussed in the panel were many topics to further encourage the use of biometric applications, highlighting NIST Special Publication SP 500-245, ANSI/NIST-ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, and Scar Mark and Tattoo (SMT) Information. The standard specifies a common format to be used to exchange fingerprint, facial, scars, mark, and tattoo identification data effectively across jurisdictional lines or between dissimilar systems made by different manufacturers. Also there were many recommendations made by the panel including the need for a single certification body for biometrics products, a need for speaker recognition interoperability standards, conformance testing methodologies for the biometric interoperability standards under development and several other issues to which accompanying recommendations were offered up to the panel for evaluations.

ANSI-HSSP Enterprise Power Security and Continuity Panel, February 2006

During the December 2004 Panel plenary meeting, the subject of enterprise power security and continuity was endorsed as one of two new areas to be explored via workshops due to its importance to homeland security. The panel discussed the use of standards and gaps therein within the power infrastructure. In February 2006 the FEMA 426 – Reference *Manual to Mitigate Potential Terrorist Attacks Against Buildings* was identified as the appropriate benchmark document for the group to use as a base model document. Over the course of the meeting the report of findings was as follows: "There is the need for a practical standard or recommended practice on how an organization should assess, plan, prioritize, etc. for overall power security and continuity. This would be aimed at both the private enterprise and entities at the municipal level. A second recommendation stresses that better private sector engagement with the public sector is needed for power security, backup, etc., both from a motivational and "how to" perspective.

ANSI-HSSP Final Workshop Report, Perimeter Security Standardization, January 2007

This workshop looked to provide guidance and assistance to standards developing organizations (SDOs) involved with standards activity for various aspects of "perimeter security," in the context of homeland security and homeland defense. The workshop report presents some basic concepts and definitions, intended to improve the clarity and precision of the following analysis and discussion. Specific concepts such as security interests (potential targets), target perimeter, security perimeter, perimeter security, attacks and threats, and risk were addressed.

Lessons Learned From Hurricane Katrina and the Role for Standards and Conformity Assessment Programs, March 2007

The objective of this ANSI Homeland Security Standards Panel (HSSP) workshop was to convene key stakeholders from both the public and private sectors to review the lessons learned and recommendations from the federal aftermath reports on Hurricane Katrina and to examine the role for standards and conformity assessment programs in assisting future preparedness, response and recovery efforts. Following a series of three meetings and intensive task group work, the workshop concluded that the American National Standard (ANS) National Fire Protection Association (NFPA) 1600, *Disaster/Emergency Management and Business Continuity Programs*, addressed the need for a high-level, voluntary standard for preparedness, response and recovery. The workshop report provided recommendations in time for consideration in NFPA 1600 (2007).

ANSI-HSSP Emergency Communications Standardization, April 2008

Following the launch of the ANSI-HSSP, the subject of emergency communications was endorsed as one of the areas that the Panel would address via a workshop. The first ANSI-HSSP Emergency Communications Workshop meeting was held December 2004. The primary standard identified as providing guidance for communications during an emergency was NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity Programs. This standard was considered along with input from the Government Accountability Office, Federal Communications Commission and other stakeholders in the subsequent discussions and outlined throughout the rest of the report.

ANSI-HSSP Internet Security Alliance, 2008

This report serves as an Action Guide that provides a practical, immediate guidance on how to bring the multiple stakeholders in cyber security together and give them, in the form of strategic questions, a roadmap for developing a multidisciplinary risk management approach to analyze, manage and mitigate the financial risks of cyber security. This document is intended for senior leadership of large entities developing a cyber presence.

ANSI-HSSP Final Workshop Report: Training Program Standardization for First Response to WMD Events, January 2009

The objective of the workshop was to identify existing training standards, training standards under development, and gap areas in training programs for first responders to CBRNE terrorist events. The standards out of this convening were focused on pre-incident planning, incident response and operations, incident command and coordination, use and care of personal protective equipment (PPE) and operational equipment, contamination mitigation and decontamination. After this workshop and several stakeholder meetings a report was handed over to the then Department of Homeland Security (DHS), Office of Domestic Preparedness as a benchmark for further development.

ANSI-HSSP Workshop on Transit Security Standardization, January 2009

In January of 2009 the ANSI-HSSP on Transit Security Standardization met with participation from the American Public Transportation Association (APTA), in order to address transit security needs. Specifically it sought to identify the following (inclusive of concept of operations): relevant standards currently published or under development, additional standards needed to aid in securing transit, performance requirements for future standards proposals, and relevant gaps in science and/or technology resulting in the findings and recommendations. Recommendations were made for credentialing, access control, and intrusion detection; explosive detection equipment; and video analytics. Following up from this workshop, outreach strategies were identified to advance these transit security standardization efforts.

ANSI-HSSP Emergency Preparedness for Persons With Disabilities and Special Needs, May 2009

On February 3-4, 2009, the ANSI-HSSP convened a Workshop on Emergency Preparedness for Persons with disabilities and special needs, bringing together over 100 key stakeholders from standards developing organizations (SDOs), federal agencies, and disability advocacy groups. The event, co-chaired by Mr. Allan Fraser, Senior Building Code Specialist, National Fire Protection Association (NFPA) and Ms. Hilary Styron, Director, National Organization on Disability, Emergency Preparedness Initiative (NOD/EPI), explored the need for standards-based solutions for more effective emergency preparedness for the community of persons with disabilities and special needs. The report outlines findings, next steps and public input.

ANSI-HSSP Standards Workshop for Non-Invasive Inspection Systems for Homeland Security, August 2010

On April 29 and 30, 2010, NIST hosted an ANSI-HSSP workshop on "Standards for Non-Invasive Inspection Systems for Homeland Security" to address the standards and conformity assessment needs for non-invasive explosives detection encompassing ionizing radiation, non-ionizing radiation, metal detectors, and automated target recognition for the security screening of persons, luggage, cargo containers and vehicles. The event was co-chaired by Mr. Lee Spanier of the Transportation Security Laboratory and Dr. Larry Hudson of NIST and was attended by 150 persons from 66 organizations representing government agencies, industry, DOE national laboratories, international partners, and standards development experts.

ANSI-HSSP Small Business Emergency Preparedness Workshop, August 2011

As part of a continuing effort to help small businesses prepare for and respond to unexpected circumstances, the American National Standards Institute (ANSI) Homeland Security Standards Panel (HSSP) convened the workshop Achieving Preparedness through Standards Implementation: Challenges and Opportunities for Small Businesses on May 25, 2011. The interactive workshop provided an opportunity for all participants to engage in an open dialogue and gain knowledge about all related issues and challenges. The event highlighted the need for preparedness, particularly for small businesses, existing standards, conformity assessment systems, and business tools that are currently in place and their value to the small business community. Challenges related to cost and duration of implementation was also covered.

ANSI-HSSP Standards for Disaster Resilience for Buildings and Physical Infrastructure Systems Workshop, November 2011

The goal of the workshop was to identify information needed to develop a framework document that will help guide the development of standards and codes for disaster resilience. It was agreed by the participants that in order to achieve resilient communities, there is a need to develop performance-based standards and codes for resilience as well as a comprehensive approach to design guidance for the built environment. Highlighted strategies were used as examples, such as the Stafford Act (Public Law 93-288).

Since the inception of the ANSI HSSP in 2003, there has been a strong effort to reach out to international partners in standards development. The workshops and the annual plenary conferences have drawn strong participation from national agencies and standards developers around the world who face the same requirements to develop rigorous standards for products and processes in the security areas referenced above.

In November 2010, ANSI hosted the Ninth Plenary Session of the HSSP (Homeland Security Standards Panel): U.S.-European Collaboration on Security Standardization Systems. Participants identified targets of opportunity for EU-U.S. standardization collaboration in the following areas:

- Aviation security
- Border and maritime security
- Conformity assessment
- Global supply chain security
- Preparedness and crisis management.

Security Standard Setting in the EU

There are three European Standards Organizations (ESOs): CEN, CENELEC, and ETSI. The mission of the European Committee for Standardization (CEN) is to foster the European economy in global trading, the welfare of European citizens, and the environment. Through its services it provides a platform for the development of European Standards and other technical specifications.

CEN is a major provider of European Standards and technical specifications. It is the only recognized European organization according to Directive 98/34/EC for the planning, drafting and adoption of European Standards in all areas of economic activity with the exception of electro-technology (European Committee for Electro-technical Standardization - CENELEC) and telecommunications (European Telecommunications Standards Institute - ETSI).

CEN is governed by a General Assembly (AG) of 31 National Members. An Administrative Board (CA) is the authorized agent of the General Assembly to direct CEN's operations. It prepares the annual budget and membership applications.

CEN signed a technical cooperation agreement (the "*Vienna Agreement*") with the International Organization for Standardization (ISO) that, in selected cases, assures the internationalization of standards.[9] Accordingly, where one of the organizations is working on a technical standard, this area will not be replicated by another organization. A similar agreement was signed in 1996 between CENELEC and the International Electrotechnical Commission (IEC), known as the "*Dresden Agreement.*"

In June 2010 the European Commission's Joint Research Centre (JRC) signed a collaboration agreement with CEN/CENELEC the objectives of which are to:

- Encourage pre-normative research and co-normative research[10]

9. The "*Vienna Agreement*" on technical cooperation was formally approved on 27 June 1991 in Vienna by the CEN Administrative Board following its approval by the ISO Executive Board at its meeting on 16 and 17 May 1991 in Geneva.
10. "Pre-normative research" is defined as R&D that is likely to generate new matters for standardization, usually in advance of these activities,

- Help support standards activities through the participation of JRC experts in CEN and CENELEC Technical Committees and their Working Groups and Workshops, and preparation of European Standards and consensus-based publications.

JRC actively participates in a wide range of CEN, CENELEC and ETSI technical working groups and associated workshops.

In order to launch a systematic process to assess existing standards, to identify gaps, and to implement new standards for security, the EU issued a Programing Mandate (hereafter, mandate) to the European standards organizations. This mandate concerns the development of a work program for the definition of European standards and other standardization deliverables in the area of security. The program takes note of all aspects linked to the different specific products, systems, procedures, and protocols that should be covered by standards to ensure that EU security is improved and consistently addressed in various security settings. The mandate concerns the analysis of the current security standards landscape in Europe and the development of a security standardization roadmap. The analysis will cover the most relevant national standards, the full range of available EU standards, as well as ISO and International Electrotecnical Commission (IEC) standards. It will cover the full range of standards types needed (some standards may cover several of these classes) to ensure protection and security of the citizen, including interoperability standards (technical, syntax, semantic, and organizational) and performance standards (establishing minimum requirements).

The mandate's work program will have to take into account security measures in line with the security levels determined by public authorities and their underlying risk assessments, as well as identifying security needs and secure interoperability schemes between the various nodes and centers for civil security in Europe dealing with law enforcement and crisis management. It should include, as well, similar needs from private perspectives.

Areas of analysis being undertaken under the mandate include the following:

- Security of the citizen (organized crime, counter terrorism, explosives, CBRN, fire hazard)
- Infrastructure security (building design, energy/transport grids, surveillance, supply chain)
- Border security (land border, sea border, air border)
- Restoring security and safety in crisis (preparedness planning, response, recovery).[11]

Recent deliberations concerning the mandate were focused on standards for interoperability and testing in the context of aviation security, cybersecurity, port security, and the protection of critical infrastructure.[12]

Until the end of 2008, the coordination in the field of security was ensured by the CEN Technical Board Working Group for Protection and Citizen Security (BT/WG 161) which functioned as a forum for this area, providing continuous networking and information exchange to keep all

(i.e., work anticipating future standards). "Co-normative research" is defined as R&D in direct interaction with ongoing and/or planned standardization activities, usually proposed by SDO technical committees (i.e., work required to progress items in the agreed program).
11. Ying Ying Lau (Secretary of CEN/TC 391), " EC Mandate on Security Standards," ANSI – ESO Conference: Transatlantic Standardization Partnerships on E-Mobility/Electric Vehicles, Energy, and Security, October 12, 2011.
12. CEN/CENELEC/ETSI Mandate M/487 to establish Security Standards and stakeholder meeting, Brussels, March 2, 2012.

partners aware of evolving activities. In December 2008, the BT transferred its activities to a new Technical Committee on Societal and Citizen Security (CEN/TC 391).[13]

The objective of CEN/TC 391 is to develop a family of European standards and standard-like documents in the Societal and Citizen Security sector including aspects of prevention, response, mitigation, continuity and recovery before, during, and after destabilizing or disruptive events. CEN/TC 391 is a forum for joint work with other CEN/TCs or other TCs where common issues are at stake.[14]

EU-U.S. Commitment to Collaboration on Security Standardization

Recognizing a long history of close partnership, shared values, and "deep interdependence," the United States and the European Commission have recently established a number of mechanisms for promoting EU-U.S. collaboration to promote greater prosperity and security for our citizens. Of particular concern here are a number of cooperative mechanisms that significantly involve EU-U.S. collaboration focused on security standardization.

The U.S. and the European Commission instituted an "Implementing Arrangement" in 2009 related to "cooperative activities in the field of homeland/civil security research." [15] This agreement extends and amends a longer standing, "Agreement for Scientific and Technological Cooperation between the Government of the United States of America and the European Community" of 1997. Section 1.7 of the Implementing Arrangement lists cooperative areas such as the

> "development and exchange of relevant requirements, standards, vulnerability assessments, interdependency analyses, certifications, best practices, guidelines, training programs, test reports, data, software, equipment, and personnel."

The Arrangement further specifies as a "nature of cooperative activities" in Section 2.1.4

> "Comparable access to laboratory facilities and Equipment and Material, for conducting scientific and technological activities including research, development, *testing and evaluation, standardization and certification; …*" [Emphasis added.]

A Steering Group is set up by the Arrangement with the Undersecretary of Science and Technology of the Department of Homeland Security (DHS) as one of its *ex officio* co-chairs. The Steering Group is authorized to "propose ad hoc activities" (Section 3.3).

In January 2009, the EU and U.S. issued a "Joint Declaration on Aviation Security," recognizing that,

> "International air transportation is a global resource on which we all rely … [and that] the European Union and the United States of America share the responsibility to prevent terrorists and serious criminals from conducting,

13. http://www.cen.eu/cen/Sectors/Sectors/Security%20and%20Defence/Security/Pages/default.aspx
14. CEN/TC 391 Business Plan Revision 02 23 Nov 2010.
15. Implementing Arrangement between The Government of the Unites States of America and The European Commission for cooperative activities in the field of homeland/civil security research," Link: http://www.dhs.gov/xlibrary/assets/sandt-implementing-arrangement.pdf.

planning, and supporting operations with the intention to cause harm to our populations including by exploiting civil aviation…"[16]

The objectives of the joint declaration include collaborating to:

- Identify individuals who pose a risk to our security by bolstering confidence in travel documents, the use of biometrics, and passenger screening
- Identify, through enhanced technologies, illicit materials destined for aircraft
- Enhance partners' aviation security capacity.

As a matter of urgency, the joint declaration sought to prepare for high-level consideration of related issues pertaining to aviation security (e.g., provision of pre-departure information to aid in screening, enhanced measures for onboard flight protection and emergency communications; and the sharing of research, expertise, and best practices concerning behavioral detection and explosives); information sharing (e.g., the functioning of, and the opportunities for, data information exchange mechanisms); research activities (e.g., cooperative research and development on physical and behavioral explosives detection and mitigation); and international activities (e.g., building capacity for screening and counter-terrorism with third countries; and the promotion of international standards in aviation security for passengers and cargo).

Collaboration in standardization for security purposes was a main point of discussion in a meeting between high-level representatives from the European Commission (EC) and DHS in early 2010.[17] It was decided to investigate possibilities for bi-lateral and cross-border co-operation in security areas. Early involvement of European Standards Organizations in these processes will offer the chance to prepare the ESOs to better understand upcoming requests and needs, and to position their constituents — users and manufacturers — to participate in the earliest stages of the standardization vision for new and improved security products and services.[18] To this end the European Commission has issued a "mandate" for the ESOs to create a security standardization roadmap of European standards for security.

As discussed in the opening "purpose" section of this paper, the European Commission's Joint Research Centre (JRC) initiated a process of U.S.-EU collaboration on security standards in April 2010, followed, in November 2010, by the Ninth Plenary Session of ANSI's HSSP: U.S.-European Collaboration on Security Standardization Systems.

In April 2011, the EU and U.S. issued a memorandum on cyber security.[19] The memorandum expressed shared commitment to deepening cooperation to address the increasing threats to global Internet and digital networks and agreed to define the issues to be tackled by the EU-U.S. Working Group on Cyber-Security and Cyber-Crime established at the EU-U.S. Summit in November 2010 (MEMO/10/597). The memorandum envisioned: expanding incident management response capabilities; a commitment to engage with the private sector; and pursuit of key issues such as fighting botnets, securing industrial control systems, and enhancing the resilience and stability of the Internet; as well as a program of joint awareness raising activities including child protection and the removal of child pornography.

16. *U.S.-EU Joint Declaration on Aviation Security*, January 21, 2010.
17. http://www.dhs.gov/ynews/releases/pr_1264119013710.shtm
18. Alois J. Sieber and Klaus Keus, *Standardization as a Contribution on the Innovation Road for Security*, mimeo, 2010.
19. "Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats," MEMO/11/246, Brussels, 14th April 2011

In May 2011, the Office of the United States Trade Representative and the Office of Management and Budget issued a joint memorandum reminding agencies of the requirement not to create "technical barriers to trade" through "standards-related activities." To satisfy this requirement of the Trade Agreements Act of 1979, the memorandum encourages international collaboration be used as a tool. The memorandum lists several practices that "should be considered (to the extent appropriate and consistent with domestic law)" by agencies:

- Information exchanges, dialogues, or meetings with other governments;
- Information exchanges, dialogues, or meetings with interested stakeholders, including SMEs, in other countries;
- Participation in efforts to share best practices and to harmonize … standards…[20]

Standards related to supply-chain security directly impact international trade. A collaborative effort between the U.S. and EU as is suggested herein will help eliminate unnecessary barriers and lower the impact of barriers deemed necessary.

In June, 2011, the EU and U.S. issued a "Joint Statement in Supply Chain Security." The joint statement makes the following claim:

> "The U.S. and the EU have the largest bilateral trade relationship and, together, account for about one-third of world trade. Other nations rely on transit through our airports, seaports and land border crossings. The partnership between the U.S. and the EU protects these vital economic ties, sets an example and promotes consensus in other organizations."

The joint statement commits the EU and U.S. to supporting the work of multilateral organizations such as the World Customs Organization (WCO), the International Civil Aviation Organization (ICAO), the International Maritime Organization (IMO), and the Universal Postal Union (UPU), especially with regard to adopting international standards and new security measures that are compatible across all modes of transport within the supply chain.

An annex to the joint statement identifies the following areas for possible action:

- Enhancing compliance with established standards
- Exploring and deploying new technologies
- Improving and exploiting risk information
- Strengthening air cargo security
- Stemming the flow of illicit and dangerous materials
- Engaging in mutual recognition of trade partnership programs and controls
- Connecting and streamlining trade partnership programs
- Building a resilient system (capable of quick recovery from major disruptions)
- Promoting capacity-building.

The EU-U.S. commitment to standardization as a means to advancing security is broad and deep. Most pledges to work together explicitly recognize the role of standards development and

20." Memorandum for the Heads of Executive Departments and Agencies and Independent Regulatory Agencies, Deputy United States Trade Representative and Administrator, Subject: Export and Trade Promotion, Public Participation, and Rulemaking," Office of Information and Regulatory Affairs, Office of Management and Budget; May 19, 2011.

implementation. All depend on the work of standards development organizations as an important path to achieving their enhanced security and citizen protection objectives.

4. The Logic of Expanding EU-U.S. Security Standardization

Providing homeland security and citizen safety has become a higher priority for all countries. In the wake of growing challenges from sponsors of terrorism, internal and external security has become increasingly inseparable. Preserving our values as an open society, including respect for fundamental rights and freedoms, while addressing the increased and diversified security threat, is a challenge for all. A recent joint report on EU-U.S. security strategies finds that policy makers in the U.S. and the EU are now focused on the internal/external security nexus. The European Security Strategy, as well as the EU's new Internal Security Strategy, argue for the dissolution of that internal/external separation, pleading for a more comprehensive security approach. The U.S. Quadrennial Homeland Security Review, as well, has brought cross-border threats into the spotlight, calling for an "integrated" approach to combating threats that cross the foreign/domestic divide.[21] It is easily demonstrated that the use of non-harmonized or security measures with different performance requirements lower the overall effectiveness of security measures. If the EU recognizes a lower performance standard than the U.S. for x-ray screening equipment, for example, a checked bag that originates in Europe will have to be rescreened again in Europe or before entering the U.S. to ensure the level of security demanded by the U.S. Protecting our openness and prosperity *requires* innovation and the efficient use of scarce resources. Standardization is an important yet often underappreciated facet of innovation and market development.[22] The overall benefits of standardization are critical to economic growth and efficiency but companies (and countries), acting alone, tend to provide less standardization than optimal.[23] It is increasingly understood that standards affect economic growth and productivity; that the use of international standards increases exports from and imports into the country that employs them; and that standards are a source of information that helps firms innovate. More specifically, it has been shown that standards can help exploit economies of scale; increase the effectiveness of the division of labor; support the building of competencies; reduce barriers to entry; induce network effects; reduce transaction costs; increase trust between trading partners; and act as important instruments in the dissemination of best practice.[24] In other words, *standards are regarded as important sources of new products and services and also the source of reduced costs for existing products and services.*

Some studies indicate that consensus standards supported by multiple suppliers are more effective than either consortium standards or proprietary standards; that they increase market share; provide opportunities to come into contact with experts who may be potential business partners; and that the cooperation with customers, competitors and other stakeholders that define common standards positively contribute to companies' reputations.[25] A recent study of the EU

21. *EU-U.S. Security Strategies, op. cit.*
22. In the U.S., the National Technology Transfer and Advancement Act (NTTAA) assigns the National Institute for Standards and Technology (NIST) responsibility for coordinating federal, state, and local government activities in voluntary standards and working with industry to develop and apply technology, measurements, and standards. NIST, in turn, works closely with the American National Standards Institute (ANSI). ANSI administers and coordinates what is, in the U.S., a voluntary private sector standardization system. ANSI is the sole U.S. representative and dues-paying member of the two major non-treaty international standards developing organizations, the ISO; and, via the U.S. National Committee (USNC), the International Electrotechnical Commission (IEC).
23. Gregory Tassey, "Standardization of Technology-Based Markets," *Research Policy*, 29, 2000, pp. 587-602; *Economics of RandD Policy*, 1997; *The Roles and Economic Impacts of Technology Infrastructure*, (mimeo), March, 2008; and *The Technology Imperative*, 2009.
24. G.M. Peter Swann, *The Economics of Standardization: An Update*, (Report for the UK Department of Business, Innovation and Skills (BIS)), May 27, 2010.
25. Henk de Vries, "Assessing Benefits: Return on Investment Soars for Participation in Standardization," *ISO Focus +*, Volume 1, No. 6, June

standardization process argues that standards facilitate cross border trade and give both buyers and sellers confidence in the quality, safety and specification of goods that comply with those standards. They also reduce "search costs" that are particularly high for buyers of imported products.[26] Policy development for international collaboration on security standardization, does not advance as fast as in other areas, but both EU and U.S. authors have developed arguments in favor of standardization in their respective purviews.[27]

Assuring that standards keep up with fast-changing requirements of product safety, quality, reliability, privacy, interoperability, performance, or security is the demanding job of standards-making organizations. Prospective business partners or customers are reluctant to commit funds to the further development or use of sophisticated products if their utility cannot be assured. Security products and services are a good example of the case that without standards the high-tech security sector would not grow in a coherent or effective way and thus would not be able to continue to address a wide variety of pressing problems in the security sector. From a European perspective,

> The market for security solutions in Europe is … highly fragmented which hinders and possibly avoids using the overall potential and accessing market opportunities in an effective way. To optimize synergy between technologies, services, stakeholders and markets, it is important to cluster the knowledge between demand and supply so as to ensure effectiveness of security solutions. Massive changes in the security market require more flexibility. Market cycles are accelerating, new developments and the importance of a global security market are rapidly increasing.[28]

A recent EU report focused on European security industry complaints about "the relative absences of industry and product standards in the security sector both in the EU and at a global level," and suggests that, "standards would facilitate both the functioning of the market in terms of interactions between suppliers and procurers/users and, also, within the industry itself." The report claims that "the development of EU standards [has] become widely recognized as a 'benchmark' in broader international markets that could strengthen the competitive position of EU suppliers."[29] The report warns that, "potential synergies within the industry may go unidentified" and "fragmentation at national levels (and even sub-national levels) can increase costs and reduce the opportunities for efficiency gains."[30]

The United States and European Union Member States have the same goal related to securing international trade and travel. That goal is ensuring security while facilitating the flow of legitimate goods and travelers. The U.S. and EU "enjoy the most integrated economic relationship in the world."[31] As robust as this relationship is, it could be stronger. The U.S. and EU should continue to work together at the bilateral level to find best practices related to trade

---

2010; also Swann, Ibid.
26. Frank A.G. den Butter and John Hudson, "Standardization and Compliance Costs: Relevant Developments at EU Level," in Nijsen et al. (eds.), *Business Regulation and Public Policy*, 2009.
27. For the U.S., see, Erik Puskar and David Leech, "Bottom-line Impact: The Economic Value of Documentary Standards," ISO*Focus+*, June 2010. For the EU, see, European Commission, Directorate-General Enterprise and Industry, *Study on the Competitiveness of the EU Security Industry*, Brussels, November, 15 2009.
28. Sieber and Keus, *op. cit.*
29. European Commission, Directorate-General Enterprise and Industry, "Study on the Competitiveness of the EU Security Industry, Brussels, November, 15 2009. (Hereafter, "EU")
30. Ibid.
31. European Union Trade, Bilateral Agreements, website: Link: http://ec.europa.eu/trade/creating-opportunities/bilateral-relations/countries/united-states/

and travel security. For example, the U.S. has recently drawn upon standards of the international community in the implementation of the Private-Sector Preparedness (PS-Prep) program administered by the Federal Emergency Management Administration (FEMA).[32] The goal of voluntary PS-Prep is to create a business community that is resilient to future disasters, natural and man-made. Voluntary consensus standards are the foundation of the program's accreditation and certification process for private sector businesses. After considering numerous standards, DHS adopted three, one of which was developed by the British Standards Institute: BSI-25999 "Business continuity management." BS-25999 remains an active standard of the PS-Prep program. [33]

Manufacturers located both in the U.S. and the EU are actively pursuing research and development to create new-and-improved devices, in many cases supported by the government agencies that will eventually employ their equipment and services. Vendors are seeking to expand current markets and open new ones. These markets are international in scope. Major customers are the agencies of national governments. The involvement of independent security standards experts early at the stage of needs identification, requirements, and capability definition is critical. Their early involvement broadens the solution space and encourages the introduction of innovative solutions. It encourages standardization at the mission need level and avoids building standards for developed products after the fact.

Having a common set of security standards at the international level is a sound strategy for the U.S. and the EU. Pooling the resources of the U.S. and EU to create these international standards will conserve resources while accomplishing the goal of a safe and secure flow of legitimate goods and travelers.

32. Title IX of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53).
33. DHS Secretary Janet Napolitano announced the adoption of the following three accepted standards for the PS-Prep program on June 15, 2010: ASIS SPC.1-2009 Organizational Resilience: Security Preparedness and Continuity Management System; British Standard 25999-2:2007 Business Continuity Management; and National Fire Protection Association 1600:2007/2010 Standard on Disaster/Emergency Management and Business Continuity Programs. http://www.fema.gov/privatesector/preparedness/adoption_standards.shtm

How Do Security Standards Create Economic Value?

Introduction

Experience shows that standards and their underlying measurement technology create value in a myriad of ways. This brief case study provides a concrete example of how security standards — in this case, x-ray standards for bulk-explosives detection — have created economic value for security equipment manufacturers, the purchasers of security equipment, and consumers of more secure transportation services. *We can expect these patterns of value creation to be replicated wherever security standards collaboration is pursued.*

Background

Since September 11, 2001 U.S. and European legislation has transformed the way in which the global air transportation system provides aviation security and caused the development of x-ray security standards for bulk-explosives detection.

Air, land, and marine transportation systems are designed for accessibility and efficiency, two characteristics that make them highly vulnerable to terrorist attack. Since the system of air travel is an international system with nodes extending beyond national borders, security concerns and actions by one nation can significantly impact the costs and/or benefits to other nations, creating a situation that demands international collaborative initiatives.

In 2001 the international community found itself with no comprehensive standards for the technical performance of x-ray or gamma-ray security-screening equipment. With the increasing deployment of such technologies for homeland-security applications, the *U.S. National Strategy for Homeland Security* (2002) identified the need for standards to support homeland security and emergency preparedness.

In 2005, NIST and the Department of Homeland Security (DHS) launched an effort to develop a suite of national voluntary consensus standards that span the use of x-rays and gamma rays in the screening of carried items and human subjects at airline checkpoints, airline checked baggage, air cargo, and other venues.

Over the course of 2007 to 2011 several of these x-ray and gamma ray standards efforts have come to fruition as national and international consensus standards. These consensus standards were developed through the participation of The U.S. Transportation Security Laboratory (TSL), x-ray equipment manufacturers, NIST, and public and private-sector researchers in national and international standards development organizations (SDOs).

Air Transportation Services

Economic value is generated by increased air transportation security. The value chain depicted below is a snapshot of the complex process by which many economic actors contribute their "ingredients" to product and services integrators further along the chain. Those contributions add value that ultimately provides more secure transportation services to air travelers and air cargo shippers — the users of air transportation services at the top of following figure.

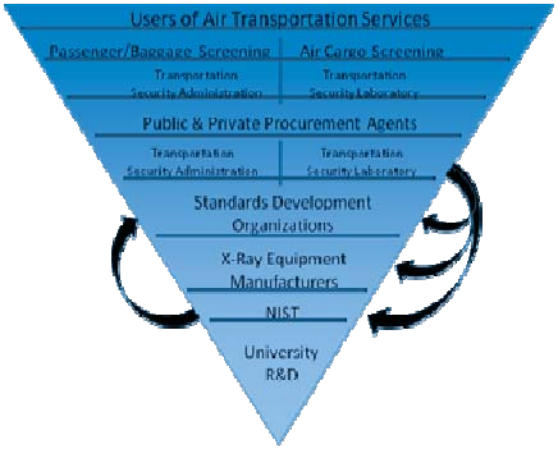

Figure 2. X-Ray Screening Value Chain

X-ray screening of passengers, baggage, and cargo is conducted across a vast air transportation infrastructure that includes some 460 U.S. airports with approximately 750 screening checkpoints and more than 2,000 screening lanes. If airline passenger traffic grows as predicted, the TSA will likely be screening over one billion people annually by 2024.

The international air transportation system transports cargo as well as passengers. Through its voluntary Certified Cargo Screening Program (CCSP), TSA also has regulatory oversight over 4,400 freight forwarders, about 300 air carriers, and more than 1,000 facilities.

As indicated in the figure above, the airlines, the TSA (supported by DHS's TSL), standards development organizations, equipment manufacturers, NIST, and university researchers all made significant contributions to the provision of more secure transportation services.

Economic Impact of Security Standards

There are three broad categories of potential beneficiaries from EU-U.S. security standards collaboration reflected in the beneficiaries of x-ray standards for bulk-explosives detection:

- End users of air transportation services
- Public and private-sector buyers of sophisticated x-ray screening equipment
- Manufacturers of x-ray screening equipment.

End User Benefits

Enhanced security has value to airline transportation services users, but competition among transportation services providers (e.g., passenger airlines) drives fares toward costs. So the typical customer will receive value above and beyond the fare actually paid ("consumer surplus").

One knowledgeable airline association representative estimated that consumers receive approximately 5% more value than they actually pay for. There were approximately 713 million airline enplanements in the U.S. in 2010. If the average price of a U.S. airline ticket was $336.00, and assuming two enplanements per trip, the total direct value of air travel ($168 x 713M) to air travel consumers in the U.S. is in the neighborhood of $20 billion. Five percent of that is approximately $1B in consumer surplus. If x-ray security standards contribute a fraction of a percent of the value of the consumer surplus airline travelers enjoy (arbitrarily, 0.0025), then the economic value attributable to x-ray security standards would be on the order of a few millions of dollars (0.05 x $20B x 0.0025 = $2.5M).

Procurement Agent Benefits

Public-and private-sector buyers of sophisticated x-ray screening equipment also benefit from the development and promulgation of consensus security standards to the extent that the standards are used by procurement agents: i.) to reduce the "search costs" required to identifying reliable suppliers and the "transaction costs" of specifying and assessing contract performance; and ii.) to encourage suppliers of x-ray screening equipment to make the investments to effectively bid on contracts for very sophisticated applications and thereby causing downward pressure on the bid prices by other suppliers.

X-ray screening equipment manufacturers estimate that competitive pressures have reduced the prices buyers would otherwise pay by 20%. There are thousands of x-ray screening machines of all types in the U.S. air transportation inventory (TSA plus those located in air cargo transportation-related facilities) with a replacement value on the order of $1.8 billion. If x-ray security standards contributed a small fraction to public and private procurement agents' ability to assess the comparative value of competing x-ray screening equipment vendors on an "apples-to-apples" basis, and induce the entry of competing firms, the economic value of that contribution would be estimated, conservatively, in the hundreds of millions of dollars. (((1.2 x $1.8B) - $1.8B) = $360M)

Equipment Manufacturer Benefits

Finally, x-ray security standards reduce the development, testing, and compliance cost of manufacturing sophisticated x-ray screening equipment. Manufacturers estimate that, on average, the development, testing, and compliance costs of sophisticated x-ray screening machines would be 40 % more costly in the absence of consensus standards. If the average unit acquisition cost of a sophisticated x-ray screening device is on the order of $300,000, and there are 6000 in the public and private inventory, a rough order-of-magnitude estimate of cost savings to manufacturers due to the availability of consensus x-ray standards would be measured in the hundreds of millions of dollars(($300K x 1.4 - $300K) 6000 units = $720M).

Summary of Economic Impacts

Based on the reasoning above, a conservative, rough order-of-magnitude estimate of the economic benefits associated with x-ray security standards are significant, possibly in the realm of hundreds of millions of dollars.

Note that this analysis primarily takes account of benefits accruing to U.S. participants in air transportation services. The greater the collaboration on consensus standards development, the broader and greater the benefits will be.

5. Expansion of U.S.-EU Security Standards Cooperation: A Summary of Benefits

Table 4 summarizes the expected benefits of increased EU-U.S. collaboration on security standards noted throughout this document. Assuring that these benefits are secured through greater collaboration will be an important management challenge for all parties involved going forward.

Table 1. Benefits of EU-U.S. Security Standards Cooperation

General Benefits	Increased security
	Increased trust between trading partners
	Identification of best practices
	Increased buyer and seller confidence in the quality, safety, and specifications of compliant products
	Increased innovation, productivity, and economic growth
	New products and services and the coherent evolution of new product sectors
	Reduced costs for existing products and services
	More effective division of labor
	Increased exports and imports
	Lower transaction costs
	Increased cross-border trade buyers and sellers
	Reduce "search costs" that are particularly high for buyers of imported products
	Increase of the potential for integrating the best research and technologies of the EU and the U.S., reducing barriers to market entry
Security-Related Benefits	**Air Transportation Services**
	End-user consumer surplus
	Lower equipment procurement costs (per unit of increasing quality)
	Lower equipment development and test costs
	Customs and Border Protection
	Improved supply-chain security
	Improved detection of contraband
	Improved inter-governmental data sharing
	More consistent policy implementation/enforcement
	Port Security
	Improved supply chain security
	Increased exchange information
	Sharing of best practices
	More consistent policy implementation/enforcement
	Crisis Management
	Improved communications
	Increased interoperability
	Increased security

6. How Will EU-U.S. Cooperation Work?

In conjunction with the European Commission's Joint Research Centre (JRC), ANSI's HSSP (Homeland Security Standards Panel) has been working to cultivate greater cooperation on security standards between the U.S. and the EU. The latest ANSI-HSSP session concluded with a pledge to identify the gaps in, and priorities for, European-U.S. collaboration; to foster the collaboration with the EU through European Standards Organizations by further dialogue on homeland security standardization; and to explore communicating the benefit of international standardization on cross-border issues.

It is envisioned that EU-U.S. security standards collaboration would proceed in a manner similar to that of the HSSP with an added emphasis on the role for early-stage innovation. In fact, during the course of the HSSP's EU-U.S. dialog, a model of joint collaboration on security standards — described as "pre-normative" standards development — has been suggested.[34,35] In this model of collaboration, standardization is an innovation activity itself. Accordingly, its advocates assert,

> The whole value of security related standards and its contribution to … innovation in security are not exhausted by a contribution limited to an isolated "after development phase." Standardization as a contribution to innovation requires a new long-term approach. One main … objective is to find ways to strengthen the alignment of research …[with] practice, including the validation of results, and to shorten the path between research and the market by standardization. Pre-normative standards —linked to pre-normative research — require the early involvement of ESOs as partners in research activities and projects. The importance of both formal and informal standards for security has to be recognized and the inclusion of new knowledge in standards has to facilitate [innovation].[36]

Sieber and Keus advocate an application-oriented "Security Scenario Profile" approach that focuses on user requirements. The approach recognizes that new security challenges entail cross-border and cross-services requirements with cascading effects across networks of systems. Unlike the traditional approach to standards development, which focuses on technology, their basic building block is a Security Scenario Profile (SSP), defined as a requirements set made of various functional "building blocks." In an airport security application, for example, "public safety" and "security screening" building blocks would map necessary functions to technological requirements, and work to develop standards supporting those requirements (similar to the x-ray screening consensus standards "virtuous circle" approach). The scenario approach is intended to help address, describe, and structure new upcoming heterogeneous security themes.

It is anticipated that as the process of EU-U.S. security standards collaboration moves forward, as technology focus areas are identified, and as the process of collaboration develops, more attention will be devoted to an organizational structure that enables significant collaboration even where the complexities — technical and political — and conflicting interests would tend to de-rail progress.

---

34. Alois J. Sieber and Klaus Keus, *op. cit.*, 2010.
35. The idea of "pre-normative standards" is similar to a "user driven" process adopted by the IT standards community during the 1980s and 1990s. It is also similar to the TSA's "virtuous circle" process desribed in section 4 above. The IT standards model is described in Robin Cowan and Georges Ferne, *Information Technology Standards: The Economic Dimension*, Committee for Information, Computers, and Communication Policy (ICCP), OECD, 1991.
36. Alois J. Sieber and Klaus Keus, *op. cit.*, 2010.

7. Possible High-Yield Areas of U.S.-EU Cooperation

Both the EU and the U.S. embrace a multi-layered security and protection concept as an organizing principle for their respective policies and activities. Both are engaged in collaborative activities to advance their security goals, and both have established forums for the exchange of information and joint activities to further the work of security standards collaboration. In the EU, the CEN/TC 391 for Societal and Citizen Security is charged with the integration of a wide range of security standardization activities. In the U.S., similar functions are being pursued by the ANSI's HSSP panel, in which EU organizations have participated. Both organizations leverage public-private collaboration to address critical security standardization needs.

Figure 3 illustrates the connection between the multi-layered security and protection framework (discussed in Section 1 of this paper) the EU and U.S. forums through which security collaboration is organized and carried forward, and the many overlapping areas of activity between them that can and should be approached collaboratively.

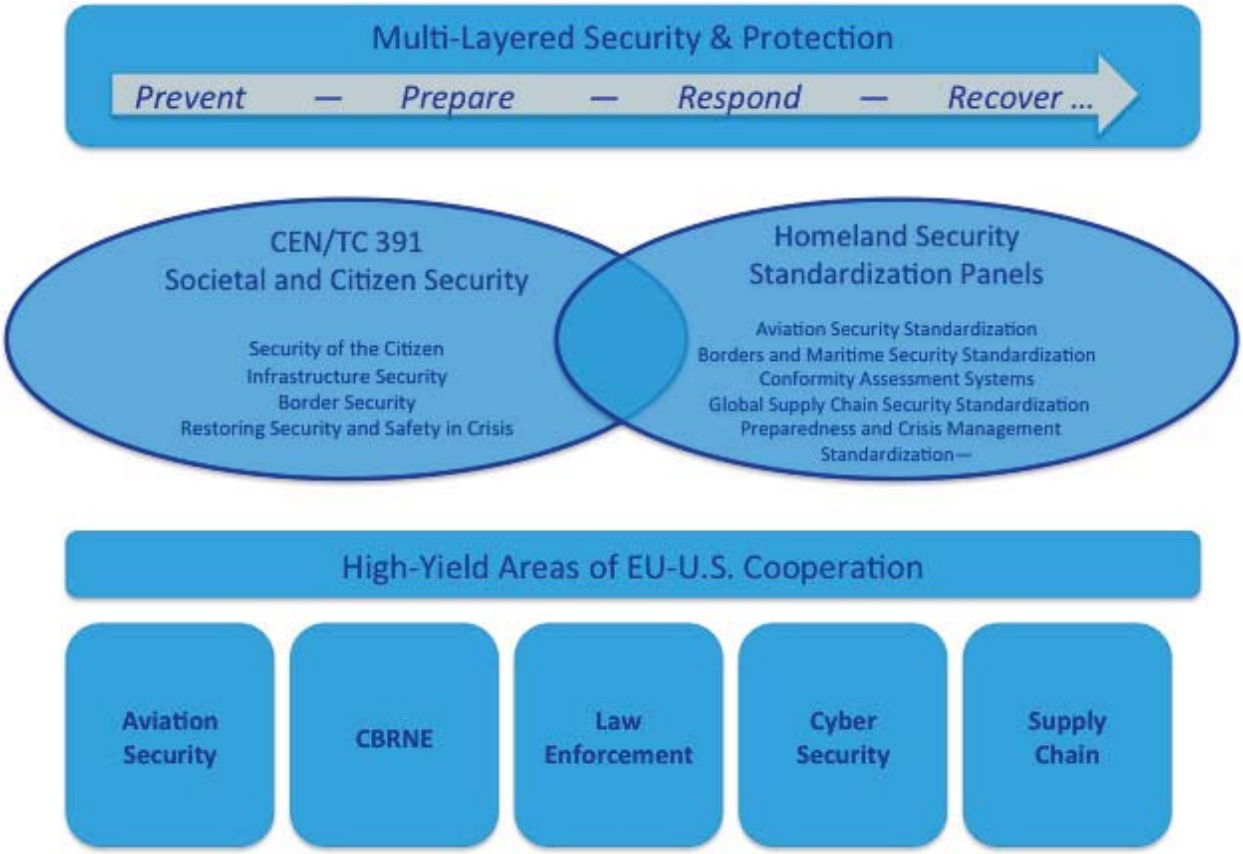

Figure 3. Overall Collaborative Security Standardization Framework

Within this broad context, several specific initiatives have been identified for cooperation including aviation security, Chemical, Biological, Radiological, Nuclear and Explosives

(CBRNE) security, supply chain security, cyber security, and law enforcement communications security.

The following are concrete examples of real-world initiatives that could be undertaken in concert by our respective standardization communities. These initiatives will not only generate technological innovations that directly meet our mutual needs for enhanced citizen security but will also instantiate our nations' high-level commitments to greater EU-U.S. security strategy integration:

WBI/AIT Image Quality Standards. It is been observed that the easiest technical standards to harmonize are those related to the newest technologies. Whole-body imaging (WBI) systems for security applications are among the newest technologies to be introduced at international aviation checkpoints. While a recent ANSI standard can be applied to gauge the technical imaging performance of x-ray advanced imaging technology (AIT), at present there are no tools to measure the imaging performance of millimeter wave-wave AIT or its relative performance to x-ray systems. Indeed, this was one of the main standards gaps identified by the April 2010 ANSI HSSP workshop on "Standards for Non-Invasive Inspection Systems for Homeland Security." The U.S. Transportation Security Administration has thus far deployed equal numbers of x-ray and millimeter wave-wave AIT machines. Due to health concerns surrounding ionizing radiation, at present only millimeter wave-wave systems are allowed in EU airports while x-ray systems undergo further review. Clearly a joint U.S. and EU standards development effort related to AIT image quality would be driven by a shared need and could result in stipulating global measurement standards for AIT. Such technical-performance standard test methods and their results would complement threat-based or operational performance testing and evaluation that produces security-sensitive information.

Biometrics. The success of biometric applications is particularly dependent on the interoperability of biometric systems. Deploying these systems requires both national and international biometric standards. In the U.S., International Committee for Information Technology Standards (INCITS) established Technical Committee M1 – Biometrics in November 2001. INCITS M1 is responsible for the "maintenance" of 24 standards as well as the accelerated development of 16 ongoing standards development projects in response to government and market requirements for open-system standards and associated conformity assessments.

One of the purposes of the U.S. National Science and Technology Council's (NSTC's) Subcommittee on Biometrics and Identity Management is to strengthen international and public sector partnerships to foster the advancement of biometric technologies. The Standards and Conformity Assessment Working Group of this subcommittee recently published a report that discusses a framework for a test and evaluation schema for biometric systems. This framework, or at least parts of it, could provide the basis for future standards that assure the cross-national interoperability of biometric systems.

Secure Interoperable Communications. Public Safety organizations and emergency responders are increasingly reliant on information and communications infrastructures and services to perform their duties; they need to collect, analyze, distribute and store information among various entities and different contexts. First responders should be able to exchange information (i.e., voice and data) in a timely manner to coordinate relief efforts and to improve the situational awareness of the environment in which they are operating.

The presence of different organizations with different communication systems often creates interoperability problems during emergency crisis. At the international level, public safety organizations employ various communications systems based on different standards: in the U.S., the main professional/private/land mobile radio (PMR) standard is APCO 25, while in Europe TETRA and TETRAPOL are the dominating standards. In addition, specific security requirements including communication and information protection and partitioning can also exacerbate the lack of interoperability. All three standards provide similar functionalities and capabilities; they require different networks and terminals (handheld and vehicular).

Security in Law Enforcement. Security incidents during disasters require cooperation between different parties and agencies, partly across borders. There is a vital need to have harmonized standards to ensure successful cooperation. To address these needs, the U.S. has NIST's Office for Law Enforcement Standardization (OLES) to foster standardization in law enforcement across U.S. agencies dealing with safety and security issues including law enforcement agencies. There is no comparable European approach. Standards for law enforcement applications are currently out of the scope of the ESOs. To strengthen the cooperation between national law enforcement agencies, supported by relevant European agencies, relevant harmonized standards need to be offered to ensure a common security level and to ensure interoperability across the borders.[37]

Chemical, Biological, Radiological, Nuclear, and Explosives Countermeasures Standards. In May of 2011 the U.S. National Science and Technology Council Committee on Homeland and National Security, Subcommittee on Standards, published, "A National Strategy for CBRNE Standards." The strategy contains a vision and six specific goals that emphasize the need for stronger interagency coordination among the nation's standards development, research, test, and evaluation infrastructure in order to achieve a comprehensive structure for coordination, establishment, and implementation of CBRNE equipment standards by 2020. The development of a complementary EU-U.S. track for such coordination would greatly enhance world CBRNE security.

We encourage further discussion about the benefits of security standards collaboration and about other high-yield areas for EU-U.S. cooperation. We invite readers to share their views. Please send comments to:

Naoma Kourti (JRC): Naoma.Kourti@ec.europa.eu

Erik Puskar (NIST): Erik.Puskar@nist.gov

37. Alois J. Sieber and Klaus Keus, *op. cit.*, 2010.