PNNL-23716

Feasibility Study of Implementing a Mobile Collaborative Information Platform for International Safeguards Inspections

September 2014

ZN Gastelum
ET Gitau
JR Doehle
CM Toomey

U.S. DEPARTMENT OF ENERGY

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

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

Printed in the United States of America

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

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

This document was printed on recycled paper.
(8/2010)

PNNL-23716

Feasibility Study of Implementing a Mobile Collaborative Information Platform for International Safeguards Inspections

ZN Gastelum
ET Gitau
JR Doehle
CM Toomey

September 2014

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

Pacific Northwest National Laboratory
Richland, Washington 99352

Summary

In response to the growing pervasiveness of mobile technologies such as tablets and smartphones, the International Atomic Energy Agency (IAEA) and the U.S. Department of Energy National Laboratories have been exploring the potential use of these platforms for international safeguards activities. Specifically of interest are information systems (software, and accompanying servers and architecture) deployed on mobile devices to increase the situational awareness and productivity of an IAEA safeguards inspector in the field, while simultaneously reducing paperwork and pack weight of safeguards equipment. Exploratory development in this area has been met with skepticism regarding the ability to overcome technology deployment challenges for IAEA safeguards equipment. This report documents research conducted to identify potential challenges for the deployment of a mobile collaborative information system to the IAEA and proposes strategies to mitigate those challenges.

Acronyms and Abbreviations

CIOSP	Common Inspection On-site Software Package
CIR	Computerized Inspection Report
COTS	commercial off-the-shelf
DIV	design information verification
DOE	U.S. Department of Energy
ECC	Equipment Coordination Committee
EMI	electromagnetic interference
FAR	Field Activities Reporting
FY	fiscal year
GPS	Global Positioning System
HPGe	high-purity germanium
IAEA	International Atomic Energy Agency
IFSS	Inspection Field Support System
INSIST	International Nuclear Safeguards Inspection Support Tool
IP	intellectual property
ISE	Integrated Safeguards Environment
IT	information technology
LTR&D Plan	Department of Safeguards' Long Term Research and Development Plan, 2012-2023
MTBF	mean-time between failure
NGSI	Next Generation Safeguards Initiative
NGSS	Next Generation Surveillance System
NRC	U.S. Nuclear Regulatory Commission
PIE	Precision Information Environment
PIE-IS	Precision Information Environment-International Safeguards
PNNL	Pacific Northwest National Laboratory
RF	radio frequency
SGIS	Division of Safeguards Information Services (IAEA)
SGTS	Safeguards Division for Technical Support (IAEA)
USB	universal serial bus
USSP	U.S. Support Program to the IAEA
VPN	virtual private network

Contents

1.0 Introduction

As part of the International Atomic Energy Agency's (IAEA's) State-Level Concept and evolution toward a safeguards system that is fully information-driven, safeguards inspectors are facing increasing responsibility at headquarters and in the field. Inspectors are expected to be familiar with, and able to act upon, a wide variety of information previously not considered during in-field verification activities related to a State, "…in order to identify proliferation indicators and assess risks at an early stage"(Gayne 2010). These new information sources include news reports, scientific literature, satellite imagery, trade data, internal IAEA data, and third-party information.

With the advances in computing and mobile technologies over the last 40 years, the IAEA has increasingly used such technology to improve safeguards implementation and to increase in-field inspector access to a growing information library. As the world migrates into an information age driven by the use of mobile devices such as smart phones and tablets, the IAEA is also moving in that direction. In the future, inspector access to information will need to span beyond desktop or laptop; computer access, including secure remote access, will include handheld mobile devices equipped with networked collaborative analytic platforms. However, the incorporation of mobile devices and their associated information systems into international safeguards regimes will undoubtedly be accompanied by concerns regarding information security, transparency, safety, and other complicating issues.

The purpose of this report is to understand the challenges that will face the implementation of mobile collaborative information systems for IAEA safeguards inspectors, as well as propose mechanisms to overcome, or at minimum lessen the impact, of those challenges. Section 2 of this report explains the motivation for the research, and Section 3 describes the research methodology of the study. Research assumptions are discussed in Section 4. The implementation barriers identified in the course of the research, and the accompanying mitigation strategies, are discussed in Section 5. The report concludes by offering recommendations for a path forward for policymakers and the research and development community interested in supporting the adoption of mobile platforms for IAEA safeguards (Section 6). Appendix A describes the IAEA Technology Adoption Process. Appendix B lists the experts the authors interviewed or convened to compile information on implementation barriers for mobile information systems and potential mitigation strategies.

2.0 Background

This section describes the increasing use of mobile devices for communication and collaboration, capabilities being developed for a mobile analysis support and information access platform for international safeguards, and the need to document potential obstacles to implement such a platform and to propose mitigation techniques.

2.1 Migration toward Mobile

The use of mobile devices for communication, information sharing, and collaboration is on the rise globally. The quantity of mobile devices in-use is forecasted to outnumber the world population in 2014—a trend that will continue as the number of mobile devices purchased daily (1.8 million smartphones, for example) is five times the global birthrate (Penny Stocks Lab 2014). This migration spans beyond the general public into communities that will have a direct impact on how the IAEA approaches its international safeguards verification activities.

The concept of providing in-field computational and data processing support to IAEA safeguards inspectors is not new. In 1990, the Inspection Field Support System (IFSS) was proposed. IFSS was a desktop or portable computer to integrate "the data required for verification and accounting so that inspectors will be able to devote more time to measurements and to derive conclusions at the site in a more timely manner" (Muller et al. 1990). IFSS intended to improve efficiency by freeing inspectors from basic arithmetical tasks, and provide on-site quality assurance and integrated data processing. However, over time inspectors became burdened by shortcomings such as (from Novatchev et al. 2010)

- Use of a disk operating system (DOS) that prevented use with newer operating systems and had limited processing power
- Software fragmentation due to modification of source code for specific facility applications requiring additional inspector training and prohibitively expensive software maintenance
- Lack of preventative, or perfective, software maintenance
- Increased need for inspector to hand perform data manipulation.

In the late 1990s, these drawbacks led to the development of the Common Inspection On-site Software Package (CIOSP) with the intent to have CIOSP ultimately replace IFSS (Novatchev et al. 2010). Currently in use by the IAEA, CIOSP is a stand-alone application installed on inspector laptops for creating sampling plans. CIOSP intakes an inventory list provided to an inspector on the first day of inspection, stratifies the list according to user criteria (in this case, type of nuclear material), and automatically creates a sampling plan. It also sends data to a local Computerized Inspection Report (CIR) system, which is uploaded to the mainframe (and, in the future, to the Integrated Safeguards Environment and Field Activities Reporting) upon inspector return to IAEA Headquarters.

Another effort in the 1990s was the International Safeguards Inspection Support Tool (INSIST), which was meant to provide an information system to "geographically organize, store, and retrieve" multimedia site and facility information used in the IAEA inspections in Iraq as well as the IAEA's environmental sampling activities under the 93+2 Programme (St. Pierre et al. 1994). While several

UNIX-based models were deployed to the IAEA for testing and evaluation, technical difficulty in maintaining the program without dedicated support staff led to its disuse.

More recently, some facility operators in the commercial nuclear industry have begun to use mobile devices to enhance communication with workers in remote parts of a plant. This has been described in trade publications (Keebler and Berger 2011) as well as made apparent via licensing requests to the U.S. Nuclear Regulatory Commission (NRC) for approval to communicate safeguards information using mobile devices.

Commercial developers of radiation detection and tamper indication equipment relevant for safeguards are also beginning to incorporate mobile devices into their systems. Examples of radiation detection equipment with mobile device interfaces include Canberra's Falcon 5000 portable high-purity germanium (HPGe) radionuclide identifier, which relies solely upon a wireless tablet for operation (Canberra). In addition, Aquila Technologies has developed a Cobra seal reader that uses the iPhone as its technical platform (IAEA 2011), although the cellular capabilities have been disabled.

Following IFSS and INSIST, the IAEA has continued to participate in this migration towards the use of mobile devices. The IAEA's interest in this area has been demonstrated via the Department of Safeguards' "Long Term Research and Development Plan, 2012-2023" (LTR&D Plan) (IAEA 2013), an internal white paper on tablets for inspections, and through an active development project of the Field Activities Reporting (FAR) program, which are described below.

The purpose of the LTR&D Plan is to describe the Department of Safeguards' longer-range needs and requirements to direct research in Member States, as well as commercial industry, while also making explicit a few activities that the IAEA will undertake internally. In the LTR&D Plan, the IAEA elucidates the following research needs potentially related to information systems deployed to mobile platforms (Milestones and page numbers of the LTR&D Plan are included):

- Integrate information sources, including satellite imagery, electronic data (including images), technical and academic literature, trade data, etc., to detect inconsistences in nuclear programs and States' declarations. (Milestone 2.1, p. 5)
- Evaluate data analysis methods and computerized tools to aid the analysis of the large amount of all-source information in order to support the State evaluation process and assist in drawing soundly based safeguards conclusions. (Milestone 2.4, p. 6)
- Deploy secure and authenticated communications between inspectors in the field and IAEA headquarters/regional offices. (Milestone 9.3, p. 8)

In addition, the IAEA has undertaken an internal effort to evaluate the use of tablets for IAEA safeguards inspectors. Recently, the Safeguards Division for Technical Support (SGTS) prepared a white paper on the potential uses for tablets by IAEA inspectors in the field. The draft white paper identified tablets as being tools primarily to "reduce…paperwork, collect measurement data, and offer the data for processing back in Vienna." The white paper identified the following areas of interest for use of tablets[1]:

[1] IAEA – International Atomic Energy Agency. 2012. "Inspection Data Tablet: DRAFT Proposal for Safeguards Inspection Equipment." Vienna, Austria

- providing a single platform for integrating NDA equipment outputs, including measurements and state-of-health information
- integrating a common electronic seals reader
- storing and displaying equipment manuals and other inspector data
- logging of attached and removed metal seals
- integrating a bar code reader for inventory verification support
- enabling a link to IAEA safeguards equipment cabinets to facilitate surveillance information review
- connecting to the Common Inspection Onsite Software Package (CIOSP) to develop electronic inventory lists and sampling plans
- linking to the Computerized Inspection Report (CIR) tool for information upload.

Finally, the IAEA's development of the FAR system demonstrates an interest and willingness to invest in mobile devices. FAR is a system under development at the IAEA to replace the CIR, and centers around shifting standalone software packages used by inspectors and staff to web-based applications that can seamlessly function on a variety of both wired and wireless devices. It is intended to include a documentation of field activities, seals, and environmental samples. The FAR project is developing a web browser-based application that will have the capability to cache data in an off-line mode so that inspectors can complete their reporting while disconnected from the Internet and then sync back to the system when a connection is available. The first roll-out of FAR, expected at the end of 2014, will be form entry only, and will not include analytical tools.

2.2 Precision Information Environment-International Safeguards

New capabilities and tools, such as the Safeguards Portal, Virtual State File, and the Geospatial Exploitation System, provide information access and analytical support for information at IAEA headquarters. However, electronic data connectivity and analysis for inspectors in the field can sometimes be challenging, depending on location. While inspectors almost always have access to a telephone (the security of which may be questionable if host-state supplied), intermittent Internet connectivity with a VPN provides the inspectors access to email and network resources. As a result, inspectors print paper documents at headquarters or download duplicate electronic files to their laptops, leading to a lack of information control and integration. This disconnect from headquarters places inspectors at risk of missing critical information to support their activities, such as the most recent news reports describing the type and scale of activities at a nuclear facility, government press releases about nuclear energy plans, or results from analytical activities completed at headquarters that were not available when the inspector departed. Real-time updates could be especially pertinent for Complementary Access activities.

In fiscal years (FY) 2013 and 2014, recognizing the need for better in-field analysis support and information access, the Next Generation Safeguards Initiative (NGSI) Safeguards Technology portfolio funded a proof-of-concept project to demonstrate the potential capabilities of an information platform system for international safeguards. This system was known as the Precision Information Environment-International Safeguards (PIE-IS). PIE-IS was based on a Precision Information Environment (PIE) developed for the U.S. Department of Homeland Security by Pacific Northwest National Laboratory (PNNL). PIE is "a secure, collaborative platform …to coordinate information collection, analysis, and

dissemination, along with logistical and tasking support, for emergency responders in the United States" (Gastelum et al. 2014). From its conception, PIE was developed to facilitate mobile-networked collaboration and analysis from a variety of stationary and mobile hardware platforms, particularly tablets.

The PIE-IS research team developed and implemented a safeguards-oriented information architecture which laid ground work for all future development. The team developed an IAEA safeguards data model, and developed the PIE server and mobile client for PIE-IS, including the following capabilities (Gastelum et al. 2014):

- automatically synchronizes data with the remote PIE-International Safeguards server
- downloads, displays and recommends task-specific information appropriate for the type of inspection or Complementary Access activity being conducted
- enables inspector to view, take, and upload photos
- enables user to search for key words and characters from photographed documents via optical character recognition software
- enables scanning of barcodes for tracking or other purposes (e.g., those applied to UF_6 cylinders)
- facilitates inspector completion of CIR
- supports progress monitoring and management of safeguards task/activity.

Though outside of currently funded work, potential future capabilities of such a system could include the potential to integrate advanced analytical support for gamma spectroscopy instrumentation, image acquisition and analysis software, and inspector logistics support.

2.3 Need for a Feasibility Study

Demonstrations of the initial PIE-IS development in FY 2013 resulted in feedback from the U.S. Department of Energy (DOE) and external reviewers that the implementation of a system like PIE-IS would be difficult or impossible. The proposed challenges in those discussions ranged from facility operational safety concerns, to information security, to operational security. Therefore, in order to fully understand and address the potential obstacles to implementation of a PIE-IS-like system for international safeguards, the research team conducted a feasibility study to document potential obstacles to implementation and to propose mitigation techniques to address them. The results of that study are published in this paper.

3.0 Research Methodology

Recognizing the increasingly pervasive trend of mobile computing technologies, the continued development of mobile collaboration and analysis platforms such as PIE-IS, and the need for improved in-field analysis tools for inspectors, it is prudent to consider what barriers these advanced platforms will face if deployed to the field by the IAEA. The collection and documentation of implementation barriers for mobile information systems, in addition to potential mitigation strategies, was completed through literature review, expert interviews, and an expert workshop.

3.1 Literature Review

The research team conducted an extensive literature review, focusing on the IAEA's technology adoption processes, mobile and wireless technology adoption at nuclear fuel cycle facilities, and the adoption of mobile technology in heavy industry (e.g., oil and gas industry).The body of literature describing potential barriers for IAEA deployment of mobile technologies, especially those equipped with collaborative information platforms, is scarce. This is because of the "newness" of mobile collaborative information platforms, as well as the limited exploration of how they might benefit IAEA safeguards. However, the research team believes that barriers from other actors deploying mobile technologies, combined with an understanding of technology deployment barriers in general for the IAEA, can help illustrate potential barriers for IAEA deployment of mobile information platforms for international safeguards.

3.2 Expert Interviews

The research team conducted in-person and phone interviews with experts with the following experience to complement information found in the literature in order to gather a broad coverage of barriers:

- former IAEA safeguards inspectors
- national regulators
- DOE national laboratory safeguards technology researchers
- former SGTS staff
- commercial vendors developing safeguards technologies.

3.3 Expert Workshop

After the barriers were identified from the literature and expert interviews, the research team held an expert workshop to achieve two goals: 1) confirm the completeness of collection and documentation of all potential barriers for deploying mobile collaborative information platforms, and 2) brainstorm potential mitigation strategies for each of the barriers identified. Experts involved in the meeting included some of those interviewed in the barrier identification process, as well as

- additional former IAEA safeguards inspectors
- former IAEA staff who worked on vulnerability assessments of safeguards technology for the IAEA
- recently separated staff from IAEA Division of Safeguards Information Services (SGIS)

- developers who work on mobile information platform activities at PNNL.

The authors will not attribute comments to specific experts in the text. However, a list of experts who participated in the interviews and the expert workshop is provided in Appendix B.

4.0 Research Assumptions

Identifying implementation barriers of a technology system that has not been fully defined is inherently difficult. Many of the potential implementation barriers depend significantly on how that technology will be used or implemented. For this report, certain assumptions were made in order to allow the research team to identify barriers without the constant caveat of "it depends." The following assumptions are based on expectations of how the IAEA would implement a mobile collaborative information platform in the near term.

1. The mobile technology adopted will be a tablet with standard accessories including a wireless keyboard. Though the same challenges will likely hold for many other mobile technologies (given the usability issues of small screens and lack of external keyboards on devices such as smartphones), it is assumed that a mobile platform adopted by the IAEA would be a tablet. Other existing and future mobile technology (smart watches, Google Glass, other wearable technology) are interesting in theory but much less likely to be adopted by the IAEA in the near-term, and are therefore outside the scope of this research.

2. Tablets will replace the inspector laptop. This means that the tablet would be required to run all software normally used on an inspector laptop, as well as interact with any equipment or other systems in the same (or improved) manner as the current IAEA inspector laptops. Initially tablets might not have the capability to run all safeguards software and thus would only be used for certain safeguards activities (for example, technical visits or Complementary Access). For those activities in which tablets are used, they will need to be in place of laptops rather than adding an additional piece of equipment to the inspector kit.

3. Tablets will not replace safeguards equipment. This study assumes that, at least in the near term, tablets will interact with (run, collect data from, etc.) detectors, but not replace existing safeguards equipment such as seal readers. It is foreseeable that a tablet could perform the functions of a seal reader; however, this would introduce additional barriers as the tablet would be required to undergo the IAEA's Safeguards Technology Adoption process. More information on this process can be found in Appendix A.

5.0 Implementation Barriers

Safeguards equipment plays a key role in the IAEA's ability to fulfill its verification mission. Thus, equipment to be used for IAEA safeguards must be highly vetted. The IAEA describes the requirements applied to safeguards equipment as follows (IAEA 2002, pp. 2-4):

> "Safeguards equipment is required to satisfy demanding functionality, usability and reliability criteria, be easily transportable and tamper-proof, provide complete and authenticated data, be adaptable to changing requirements, be available in the required quantities at an affordable cost, be able to be cost effectively implemented in demanding nuclear environments, be compatible with other safeguards equipment and be compatible with the capabilities and training of staff. …All aspects of equipment performance are evaluated [by the IAEA], including compliance with specifications, reliability, transportability and, most importantly, suitability for use by IAEA inspectors in nuclear facilities."

This process would be prohibitively slow for deploying collaborative mobile information platforms for IAEA safeguards. Fortunately, if the systems were used in the same capacity as IAEA laptops, they might not have to undergo this procedure. Current practice for new laptop adoption by the Department of Safeguards is review by the Department's Office of Information and Communication Systems, focusing on capability and price.[1]

While the deployment of tablets is expected to face some challenges that have already been addressed by the IAEA with their use of inspector laptops in the field, some technology deployment barriers will be unique to tablets. In this section, we will introduce barriers to the implementation and deployment of collaborative mobile information platforms for IAEA safeguards. Many of the barriers identified in this section have parallels to the IAEA's use of laptops and are not new. Those barriers that are unique to mobile platforms will be emphasized.

5.1 Safety

The IAEA's implementation of collaborative mobile information platforms potentially will be affected by two safety considerations: safety of the use of a piece of equipment at a specific facility, and inspector or personnel safety while operating that equipment in any given environment.

5.1.1 Facility Safety

Inspector use of tablets within a facility should not pose significantly increased risk over a laptop. If inspectors will take tablets into areas in which laptops were not previously used, safety issues will come under closer scrutiny.

All equipment and instrumentation introduced into a nuclear facility must ensure that the fundamental safety systems of the facility are not exposed to undue risks. These safety systems are those that ensure

[1] If a mobile device were to replace a piece of safeguards equipment such as a seals reader, though, it would likely have to go through the full authorization process.

control of reactivity, removal of heat, and confinement of radioactive material due to planned or accidental radioactive releases. Included in these systems are major physical apparatuses (e.g. control rods in a nuclear reactor), as well as supporting components like instrumentation used to monitor their status (IAEA 2012). It must be ensured that new equipment will not inhibit any part of these systems' functionality.

Interaction between a tablet and a facility's safety system would be incredibly limited. While it may be possible for the wireless platform to use a facility power supply that also provides power to safety systems, it is reasonable to assume that a mobile platform used by an inspector would never be connected to a system or instrumentation considered critical to the continued operation of safety systems at a facility. Furthermore, the function of equipment installed, or used by the IAEA through joint-use equipment agreements, would not serve a critical safety function. As such, the largest facility safety barrier to the deployment of a mobile platform is likely the potential for electromagnetic interference (EMI). Interaction between the platform and critical safety systems could also occur if a facility wireless network is used to connect the inspector's device with IAEA headquarters.

5.1.2 Personnel and Inspector Safety

For safeguards equipment, the IAEA conducts safety tests to ensure that the operation of the equipment will not pose safety hazards to inspectors or other staff as part of their safeguards equipment adoption process.[1] However, tablets being used in lieu of laptops will not likely undergo the same rigor of testing. Yet, because of their high mobility, tablets or other mobile devices may introduce additional personnel safety hazards compared to laptops. Specifically, tablets are more likely to be used while walking, climbing, or in combination with other tasks while laptops are generally used either in the IAEA office or during stationary measurements.

In some instances—such as protecting themselves against electrical shock from an unground power supply (IAEA 2003, section 3.5.4.7) or working in a facility with contamination hazards—inspectors and staff will wear rubber gloves and protective eyewear. Input devices for any mobile platform must consider what impact gloves will have on the ability of an inspector to operate the device. Protective eyewear may introduce additional glare, inhibiting the ability of the inspector to safely operate equipment.

[1]This process incudes: Potential safety hazards associated with the operation of equipment by inspectors or other Agency staff must be considered. For safeguards equipment, a safety evaluation is performed to ensure that equipment systems "are as free as possible from work-related health and safety hazards that might cause injury or illness." (IAEA 2003, section 4.2.2.3). IAEA staff members are not allowed to use safeguards equipment at facility unless the equipment has been approved for use in Category A or B. Detailed safety-related requirements are maintained by SGTS. However, several demonstrative safety barriers have been drawn from the literature and expert interviews. The IAEA ensures that equipment and instruments present no electrical hazards. This includes internal electrical hazards, such as electrical shorts, but also external hazards such as compatibility between facility power receptacles and equipment plugs. If not compatible, the IAEA considers what converters are necessary to ensure safe operation (IAEA 2003, section 3.5.4.7). Additionally, any equipment with internal or external moving components destined for use in an inspector's hand needs to be evaluated to ensure excessive vibrations do not result from use, limiting usability and potentially increasing inspector fatigue. Furthermore, equipment with external moving components may have pinch points that must be identified. Equipment that incorporates sound must be evaluated to ensure noise levels are not excessive and can be heard through any necessary auditory personal protective equipment that may be needed inside a facility.

The device must be able to function safely within the operating environments in which IAEA inspectors often find themselves. Examples of such conditions include temperatures over 40 C (104 F), high humidity, tight areas or spaces within a facility, or the need to traverse a ladder or stairs with equipment. Additionally, in facilities with contamination hazards, protection of the mobile device must be considered. For example, if the inspector carries a tablet into a processing area, a protective covering may be necessary to ensure the device does not become contaminated. If a piece of equipment becomes contaminated, swipe samples of all its surfaces may be required before it is certified (either by the operator or the IAEA) as safe. The design of some equipment, such as a keyboard, might be prohibitive to sampling all surfaces after decontamination, and must be considered prior to introducing equipment that will be regularly removed from facilities where contamination may pose an issue.

5.1.3 Safety Mitigation Strategies

The safety restrictions that may apply to a tablet will be highly facility-specific. In some facilities, there will be requirements related to what frequency a device can operate on. In cases where radio frequency interference is an issue, protective covers or Faraday shield may be used to limit radio frequency (RF) interference. Bluetooth or other close-proximity syncing, rather than longer range wireless technologies, might also eliminate some of the potential RF interferences.

Modular models for data transfer would be another strategy for addressing RF interference concerns. In a modular model, a device which stays at the host facility can sync data with a tablet when the two are close, and the tablet could then sync with IAEA headquarters over a secure Internet connection, perhaps outside the facility.

For tripping, ladder, and other mobility hazards, a safety wrist strap might help. This same consideration must be given to items required to operate a device. In the case of a tablet that requires a stylus, physically attaching the stylus to the tablet may be necessary to eliminate safety hazards. In a more forward-looking situation, wearable technologies such as smart watches that are gesture-driven might eliminate some of the hazards related to walking while operating a device that could limit visibility.

5.2 Security

Inspector processing and storage of States' safeguards information or other State- and facility-specific data in the field have always posed an information security risk. Yet, the introduction of collaborative mobile information platforms could heighten that risk if information is transmitted wirelessly back to IAEA headquarters while the inspector is in the field. In addition, the small size (and thus ease with which many mobile devices can be lost or stolen) poses additional operational security risk that must be addressed prior to IAEA deployment of such systems.

5.2.1 Operational Security

One interviewee stressed the operational security issues that might be posed by a mobile device. Information about the current location or planned activities of an IAEA inspector can be sensitive, especially for short-notice random inspections and no-notice random inspections. If a mobile device was lost, stolen, or hacked, information could be compromised regarding current location, or forthcoming inspections. This is a barrier that is already being faced (though perhaps to a lesser extent) with inspector

laptops as well as IAEA-issued smart phones which have connectivity to email and IAEA networks via VPN (though inspectors are discouraged from downloading network documents to their phones). A mobile device for IAEA safeguards would need to prove that this security risk is minimal on any device that would be deployed.

5.2.2 Information Security

The transmission of safeguards data over a wireless network poses increased information security risks compared to the current practice of transmission over hard lines or waiting for data transfer until an inspector is back at IAEA headquarters. This is because wireless networks are inherently more difficult to secure than physical connections (Farris and Medema 2012; Peterson et al 2007). Several interviewees echoed this point, noting that one barrier to deployment would be a demonstration of high levels of information security on the device so that it could be used with potentially unsecure networks and Internet connections.

One expert interviewed for this project said there are potential data security issues when inspectors are on travel for extended periods, conducting inspections in multiple countries. The inspectors will carry the information they need for all the inspections with them, including safeguards confidential information about each State. State safeguards information can be an enticing target for acquisition by other States in which the inspector is conducting activities. This is especially true when traveling between States with poor diplomatic relations. One former inspector noted that keeping sensitive information with inspectors in the field was difficult (e.g., Do you take papers with you to dinner?). Some of the difficulty in physically maintaining information security can be reduced by the inspector having all information located in a small computing device rather than stacks of papers. However, the digital information security risks are substantially increased.

In addition, if the mobile device would connect to IAEA safeguards equipment (for example, the Electo-Optical Sealing System (EOSS)), it may need to store authentication keys required to authenticate it to the equipment. There may also be cryptographic keys used to sign data or to connect over the VPN. If an inspector connects a mobile device to a host State network for any reason, that device and its information become vulnerable to whatever malicious activity may occur on that network. Most likely, an inspector would be connecting to a host State network to access the Internet, for data transfer to or from IAEA headquarters. In this case, pertinent information security threats are observation and manipulation of those data. Because the host nation has control of all the hardware and software links between the inspector's device and the gateway device for the Internet, it is possible for the State to implement malicious capabilities to observe and/or alter the outgoing or incoming data.

Apart from the threat to data in transit, the information in storage on the device is also vulnerable. Whether using a remote attack or malware installed on the device, a malicious actor able to gain access to the mobile device could observe and alter resident data. By connecting to a State-hosted network, a device becomes vulnerable to whatever remote attack or malware installation methods an actor can execute in that environment.

A State's capability to secure its own network plays a key role in determining how widespread the threat space is. If the host State has advanced capabilities in information security and it can secure its network effectively, the risk to the inspector's device is more likely to come from malicious activity of the State. However, if the state has more rudimentary information technology (IT) capabilities—

particularly with respect to security—then the threat space is more likely to include other actors who have been able to penetrate that State's network. This could include other States as well as non-state actors that would like to be privy to, or be able to alter, confidential safeguards data.

As is the nature of information security threats in the Internet-connected systems in which most devices operate today, the information security threat to a single inspector's device follows it to other networks to which it connects. Namely, if a mobile device is compromised in the field and malicious software is installed, the device can transfer that malware to other networks it accesses, whether in other States or at IAEA headquarters. This can cause the inspector to be an inadvertent information security risk for the data of the States in which he or she inspects, allowing malicious actors to now access the data on devices in their network. This can also cause a larger information security problem for the IAEA if the malware is transferred to devices on the headquarters network when the inspector connects the device upon returning from the field.

One interesting perspective on security came from an interviewee who said that users are the primary security risk for mobile information platforms. Namely, effective security protections can be put in place but it is still possible for users to take actions that expose devices to malicious actors. Currently, IAEA inspectors bring laptops or other mobile devices with them in order to interface with equipment, write reports, and conduct other inspection functions. However, they use those same laptops for watching movies, visiting websites, downloading games, and communicating home. Inspectors using an IAEA mobile device for personal use or installing unapproved or untested software and updates on the device can open the device to exploitation and expose safeguards data on the device to malicious actors. These user actions can inadvertently open the device to attack even when device-based security protections are implemented, making user actions on the device a critical security risk.

Finally, the deployment of a mobile information platform for IAEA safeguards would have to integrate with the IAEA's Integrated Safeguards Environment (ISE), a secure computing system. ISE was originally envisioned as an air-gapped system which would store all safeguards data and analytic tools. Problems getting data onto and off of the system has led to reconsideration of the air-gap. ISE is still intended to be a master repository for all safeguards data, and there are several projects and groups within the Department of Safeguards that use ISE as a data repository. Yet, how ISE ultimately will be used for IAEA safeguards data and programs is still evolving, and thus its impact on the deployment of a mobile collaborative information platform cannot be determined yet.

It is important to note here that these information security barriers for implementation are not unique to tablets. All of the considerations in this section apply to laptops as well, and these devices are already in use by IAEA inspectors around the world. With respect to absolute vulnerability to information security threats, each device will vary based on its hardware and software platform and configuration, and there could be some difference between laptops and tablets in that sense. However, the categories of vulnerabilities and techniques for mitigating them are largely the same. Depending on how mobile devices would be used, there could be a higher vulnerability to be considered. For instance, given its design, a tablet could be seen as more likely to need to use wireless connections than a laptop. If wireless connections use increases with tablets versus laptops, then the vulnerability to information security threats would also increase with that transition. Overall, however, this barrier to implementation should not be seen as prohibitive.

5.2.3 Security Mitigation Strategies

Given that the implementation concerns of security are not unique to tablets, only perhaps heightened in some respects, they are already being addressed by the IAEA in its use of laptops. Similar steps can be taken to mitigate risks in security of mobile devices.

IAEA laptops are equipped with system-wide encryption in which the full disk is encrypted upon hibernation or shutdown, and only the files currently being accessed are unencrypted while in use. Disk encryption is a feature common to most major tablet platforms today as well. The specifics of the technical implementation can vary, so the IAEA would need to consider which platform would fit its needs. However, deploying a mobile device with encryption for stored data should not be a difficult goal to meet.

Additionally, there are application-based and manufacturer- and service-provider-based methods to allow a user to remotely wipe the data from a mobile device via a Wi-Fi or cellular data connection. In this way, if a mobile device is stolen, the IAEA can remotely delete all the data from the device, ensuring that operational and information security is maintained and sensitive and proprietary data are not viewed by any unintended parties. Another mitigation option for erasing an "offline" device would be to implement a mandatory connection period to the IAEA network, for example five days, or input a security code like that of an RSA token, if network connectivity is not an option. Either option would reset the "erase device" command. If neither the device was connected nor the security code entered, the device would automatically be erased. In this manner a stolen or lost device would be guaranteed to be wiped even if the device was never connected to a Wi-Fi or cellular data connection. While wiping data from the device would likely be the primary concern in the case of theft, there are also plenty of software-based methods for tracking a stolen device. In this way, a mobile device possibly could be recovered after a theft.

With respect to accessing an unsecure wireless network, encryption again will be critical to providing security. In this case, end-to-end encryption of the connection from the device to IAEA headquarters will be a mandatory step. This can be accomplished using a VPN connection implemented via software at the device and at headquarters. A VPN provides a secure tunnel within the unsecure network connection in which all the content sent and received is encrypted. This could prevent observation and manipulation of the data being transferred. This technology is already in place for use with IAEA laptops in the field, as well as for IAEA smart phones to access email. The IAEA would simply need to ensure that the particular platform they choose is able to support the particular VPN technology they would like to use.

However, connecting to an unknown network is still a security concern, and conscientious information security practices need to be followed. Operating system and software patches and updates need to be executed in a timely manner. Devices need to be configured with secure settings that prevent unintended—and possibly malicious—actions and limit access to data by users and applications. Depending on the platform selected, antivirus protection software should also be installed.

Controlling user actions on the device will be of high importance because, as we noted, users represent a critical vulnerability when implementing security controls. Currently, inspectors are able to use their business laptops for both official and personal use. The goal with introduction of a mobile device would be to replace laptop capability and streamline inspector activities. As such, it would be the intention to have the tablet be the sole computing device an inspector would need to take into the field. It

is anticipated that inspectors likely still would desire to use the device for personal use. It would be prudent to control what applications may be installed on the device.

The current method for enabling protection of sensitive data while allowing personal use of laptops is to have a hard drive partitioned dual-boot enabled. This physically separates the business data from personal data and prevents access to confidential safeguards information when using the laptop from the personal side. In this way, if an inspector's actions cause the laptop to become vulnerable (e.g., inadvertently downloading malware), a malicious actor will be unable to access the sensitive data. Hard drive partitioned dual-booting is not a common practice with tablets and is less feasible as a solution. However, there are software-based partitions that can effectively separate data and applications on a mobile device into business and personal use. One example is Samsung Knox, which is a virtualization technology for the Android operating system. It works at the operating system level to separate applications and data within the virtualized environment from those outside it. The IAEA could use this type of system to install approved safeguards applications and store all confidential data inside a secure environment, and allow an inspector to switch to the other environment for personal use.

The innate security models and available security additions (through software, etc.) of mobile devices and operating systems vary. The IAEA will need to consider these options and weigh them against other concerns such as IAEA's ability to manipulate the functionality of the devices and how much collaboration with device manufacturers will be necessary to deploy and sustain the platform. Regardless of the security policies and technologies that are put in place, it is critical that inspectors continue to be trained on best information security practices. This would include what the IAEA security policies are, how to use the implemented security technology effectively, and how to operate in a secure manner on connected devices—whether personally or professionally. The international work environment of the IAEA compounds this challenge, in which staff members have different levels of personal and professional history with security practices, as well as various cultural norms and values regarding security.

5.3 Cost

There will always be a cost associated with investigating and implementing a new technology (Farris and Medema 2012). The IAEA has recognized the potential of cost prohibitions for engaging new technologies, and calls out two components of cost: development cost and support cost. According to the IAEA, "Development is accomplished primarily through Member State Support Programmes…Support is provided by in-house human and facility resources for services such as installation, testing and commissioning, set-up and calibration, inspector training, maintenance and repair, and inventory management" (IAEA 2002, pp. 3-4). Testing a new technology can also be costly, and time consuming. One interviewee noted that if new technologies cost close to the previous system, people would continue to use the previous system. There will also be cost associated with the development of wireless networks and related infrastructure needed for the deployment of collaborative information platforms, though those costs will likely be borne by the Member States.

While there is some cost associated with the deployment of mobile collaborative information platforms for IAEA safeguards, most of those costs would replace cost incurred via the increased use of laptops (software development, hardware costs, etc.). Depending on the selected platform, there may be some software development costs to get existing IAEA safeguards programs to work on a tablet. In

particular, if an Android or Apple tablet were chosen, existing software would need to be re-engineered to work on these platforms. If a Windows Pro tablet (running a full version of Windows) were chosen, porting existing software should require little to no refactoring. The required testing and adjustment effort would be the same as verifying software compatibility for a standard Windows operating system upgrade.

For existing web applications, moving to a mobile platform—regardless of operating system—would be quite simple. The Agency would only need to do testing and minor modifications to ensure that the software functioned correctly in the Web browser of the selected device. In total, the cost of safeguards applications running on a tablet is not expected to be significantly increased over current laptop use costs.

5.3.1 Cost Mitigation Strategies

Cost of a mobile collaborative information platform can vary considerably based on the device used and the quantities needed. However, the scale of the costs of mobile platforms such as tablets is fairly inconsequential compared to other IAEA measurement systems. Despite the very limited IAEA budget for safeguards technologies, most interviewees did not consider the cost of a mobile collaborative information system to be a significant barrier for IAEA deployment. Costs might also be minimized by coordinating external development of a collaborative mobile information platform with ongoing IAEA activities for mobile platforms such as FAR.

5.4 Infrastructure

Infrastructure refers to the basic technological systems that are required to be in place at a facility in order to have the most effective use of tablets. Many of these systems are also required (though, not necessarily in the exact form) for inspector laptops. Operating modalities of a tablet running a safeguards application (such as off-line caching) may also decrease the impact of some of these barriers. For the purpose of this research, infrastructure barriers to the deployment of collaborative information platforms are concentrated in three areas: connectivity, power supply, and data storage.

5.4.1 Wireless Connectivity and Internet Infrastructure

Wireless connectivity at a facility will pose similar barriers for either an inspector laptop, or a mobile device such as a tablet. However, because of the assumed use of tablets to transmit data back to IAEA headquarters prior to returning to Vienna, Internet connectivity may have a larger impact on mobile collaborative information platforms than the current method of inspector laptop use.

While not required for most systems, a mobile collaborative information platform would ideally be capable of transmitting and receiving secure communications from inside a facility. On-site connectivity would involve either connecting to a facility's wireless Internet network (with operator permission), connecting to an IAEA-installed wireless Internet (may be prohibitively complicated and expensive for established facilities), or periodically manually connecting to an Ethernet connection (which would require an adaptor for most tablets). Several nuclear power plants around the world have begun to consider the application of wireless networks for their facility use (Farris and Medema 2012). However, one expert indicated that inspectors would be unlikely to connect to an internal network because the risks associated with the security of such systems, as detailed above. Furthermore, some countries do not have

the necessary human capital to install or maintain a network robust enough for real-time communication between inspectors and IAEA headquarters.

5.4.2 Power Supply

Most mobile devices may be powered either via battery or direct connection to an energy source, and are intended to run mostly via battery. If tablets or other mobile platforms replace inspector laptops, dependence on battery power is not expected to pose a significant barrier to implementation as tablets and laptops have comparable battery lives. Operational conditions may allow for charging tablets on-site (note that some mobile device batteries are charged via a universal serial bus (USB) port on a laptop and would require the ability to charge via an electrical outlet).

If a mobile device will be charged at a facility, the IAEA must consider the compatibility of their equipment plugs with power receptacles at a facility. This means not only compatibility of the physical plug type, but also the transmission voltage and frequency. The IAEA may have to identify a proper adaptor or converter for equipment, request that a compatible receptacle be installed in a facility, or replace the plug on installed or to-be installed, equipment (IAEA 2003, section 3.5.4.7). This should minimally impact to IAEA safeguards inspectors, as they are already using equipment in many different countries and most tablets are compatible with voltage and frequency ranges required for global use.

5.4.3 Data Storage

If tablets are to be used to collect and process safeguards information, data storage must be considered. As with current inspector use of laptops in the field, the data collected and transmitted using a collaborative mobile information platform must be transferred back to IAEA headquarters either remotely using the Internet, or once the inspector returns to Vienna.

The size of onboard storage available on mobile devices should be considered. Mobile devices are typically equipped with much smaller amounts of onboard data storage than laptops. If data is only stored locally on a device for the most immediate inspection activities, this is unlikely to be a major issue. Considerations of how much data an inspector will be able to store before needing to “offload” to IAEA headquarters servers or to external storage media should be addressed when selecting a mobile device for deployment.

5.4.4 Infrastructure Mitigation Strategies

In relation to a site’s wireless infrastructure, the IAEA inspector should plan on relying on Member State infrastructure as little as possible. This approach can go as far as limiting Internet connections to situations in which VPN is available, or foregoing the use of the State-supplied wireless Internet connection completely, until a time when a trusted connection becomes available. Reliance on a Member State’s wireless internet could be overcome if the mobile platform relied upon cellular or satellite communications. However, emission of these types of signals through facility infrastructure (such as containment walls) will present challenges. Some tablets also offer the option to connect through Ethernet via a USB modem. This option would allow a device to use a hardwired connection that may already be available to an inspector laptop or other piece of connected equipment, and would alleviate the need for a wireless connection, provided the tablet had sufficient onboard caching capability for collected data.

With respect to power supply, many vendors design their mobile platforms to be flexible to operate across varying environments, given the international markets that they are targeting. This provides an advantage for the IAEA in overcoming this barrier. Another means of addressing the issue of power infrastructure is reliance on spare batteries. However, that strategy can bring its own difficulties and concerns, including operator acceptance of hazards, such as the chemical composition of the internal acid or liquid of a battery, physical size limits (e.g., portability), capacity, and lifetime and reliability.

Finally, secure backup and encrypted transmission to IAEA headquarters could alleviate some risk of data loss from system crashes and lost or stolen tablets. Secure backup would improve upon current practice of downloading data to removable storage media, which poses information security risks.

5.5 Information Architecture

Information architecture refers to the structure of the data model, analytical tools, permissions, and processes that compose an information system. The use of a mobile collaborative information platform in the field, with IAEA inspectors feeding real-time data back to analysts or technicians at headquarters and vice-versa assumes certain characteristics of an IAEA information architecture. These include allowing for streaming data and multi-user concurrent access and modification of files and databases. The data transmission method and timing also must be considered—whether data will be sent from the system as a single, large file, or in multiple pieces or packets.

These data acquisition, manipulation, and synchronization considerations are critical for the effective functioning of a distributed collaborative platform. Correct implementation of this architecture is fundamental for the information system aspect of a mobile device deployment. These capabilities would need to be added to and integrated with existing information system architecture at IAEA headquarters. This information architecture would also need to appropriately interface with existing technology, information systems, and measurement equipment currently installed at facilities or carried by IAEA inspectors.

5.5.1 Information Architecture Mitigation Strategies

In designing the information architecture, characteristics such as ability to stream data, multi-user concurrent access, and modification of files are more considerations that must be made. These are capabilities that already exist commercially. Streaming data are of course a component of many web- and network-based applications. Concurrent access and modification capabilities can be seen in products such as Google Docs, where multiple users can make edits to the same document at the same time. Additionally, major database software providers have effectively implemented the logic for managing concurrent user access and manipulation of files. These are not new problems but they are components of the architecture that must be recognized ahead of time and built into a collaborative mobile information platform.

While connecting to ISE will likely be a challenge, the IAEA must determine how ISE will be used prior to the team developing mitigation strategies for this challenge. Potential solutions, based on theoretical implementations of ISE, include document syncing only when connected to the ISE system at headquarters, or transmission of non-sensitive data via the system, operating external to ISE. The use of

ISE and its impact on information sharing, transmission, and collaboration, is something that will affect any system interacting with IAEA safeguards data, including inspector laptops.

5.6 Sustainability

Sustainability was raised repeatedly in the literature and in expert interviews as a key barrier to deployment of a collaborative information platform. Sustainability concerns took two forms: software and hardware. Sustainability was especially important because of the long deployment period of IAEA technologies—usually 5-15 years, so being able to access replacement parts and update code as needed with security patches or to accommodate new operating systems is highly desirable.

5.6.1 Software Sustainability

For software, sustainability barriers relate to the maintenance and upgrades of software in order to maintain secure operations and functionality throughout the expected lifecycle of the software. This includes potential interaction with frequent operating system updates or upgrades, as well as interactions with new equipment. Sustainability has posed a significant barrier in historical deployments of DOE national laboratory technologies to the IAEA because source code has stayed with the developing laboratory, which means that the IAEA was required to go through the channels of the U.S. Support Program to the IAEA (USSP) for updates (either capability-based or for interoperability with new software and operating systems) and upgrades. Historical experience with the IAEA and national laboratories has shown that when an update is needed, the logistics required to go through the USSP to the IAEA (which would then go back to the laboratory originator, who, in some cases, may have retired or otherwise left the laboratory) is not an efficient solution.

5.6.2 Hardware Sustainability

For hardware, the deployment cycle of IAEA technologies and the quick rate at which mobile platforms are advancing and changing forms means that deployment of IT to IAEA inspectors has the potential to become outdated even before it can be deployed. Koskelo and Kadner (2011) claim that this deployment of technologies that are already 5-10 years behind the state of the art will likely lead to obsolete systems. This would be an impediment for trying to maintain an effective and efficient system. Obsolete hardware also would cause difficulty in maintenance and replacement. If a system is outdated by the time it is deployed, then being able to repair or replace parts or an entire device to maintain the system will be challenging—especially if they are no longer in commercial production.

5.6.3 Sustainability Mitigation Strategies

In order to better handle software sustainability for a collaborative mobile information platform, the IAEA may require ownership of the source code and intellectual property (IP) rights. According to Koskelo and Kadner (2011), the turnover of source code and IP rights has the potential to become contentious for some organizations. For companies that are stable, well-known IAEA vendors, ownership of IP may be a less stringent requirement than for others. There has also been discussion about the potential to use open source software in order to mitigate the source code ownership issues.

In order to avoid some of these deployment and sustainability hurdles, the IAEA often relies on commercial off-the-shelf (COTS) products from reputable, stable vendors. The acquisition and deployment of a system can then sometimes be more straightforward than that of highly customized national laboratory solutions.[1] The use of COTS allows the IAEA to maintain a system for which upkeep is less complicated by bureaucratic and personnel factors avoidable by working with commercial organizations. If the IAEA is to widely deploy a mobile collaborative information platform, it will be critical to work with organizations that can sustainably develop and maintain it.

Peterson et al. (2007) echo the preference for standardized versus proprietary systems for the oil and gas industry, noting that the use of standardized systems "…provides the industry with the freedom to choose between suppliers with guaranteed interoperability. Due to this, standardized systems usually have a much longer lifespan than proprietary solutions…" (Peterson et al. 2007, p. 221), though they do concede that going through the process of international standardization can be time consuming, meaning that proprietary systems may be available sooner than their standardized counterparts.

Hardware components for a mobile platform deployed to the IAEA should be straightforward to assemble and easy to find. Regional availability should be considered. For example, hardware should rely on metric-sized parts and components rather than the English-sized components because they are more readily acquired in Vienna and other parts of the world. To address problems of future availability of replacement parts, some vendors (and occasionally the IAEA itself) will stockpile components or have out-of-production parts specially made for needed replacements. Technology developers might also consider using "bleeding edge" technologies because they could have longer shelf availability than current widely used parts, though they carry additional risk that they will not be widely adopted and therefore less available in the future. These options will need to be weighed when evaluating the sustainability of the hardware in any mobile platform solution.

5.7 Regulatory Compliance and Facility Policy

The existence of wireless networks and mobile information platforms such as tablets and smartphones are more recent than many facilities' operating licenses with their national regulators. As facilities begin to explore the implementation of wireless networks to support their operations as well as to support

[1] There has been extended discussion regarding the need for the IAEA to seek software developed by main-stream commercial vendors, rather than national laboratories or other highly specialized scientific organizations, specifically to support software sustainability. However, such specialized organizations are likely the only ones with the knowledge, mandate, and flexibility to develop and test such systems. Yet, the current engagement paradigm between the IAEA and the DOE national laboratories restricts potential collaboration and reach-back for support or updates to software. Collaboration between DOE national laboratories and the commercial firms that have successfully sustained IAEA market sectors could yield a mutually beneficial way to commercialize and deploy software and mobile device to the IAEA. In any case, the role in which the laboratories can support IAEA development and deployment of a mobile collaborative information platform should be well-defined and based on the organizations' strengths and capabilities. This could include lab-led thought pieces on potential desired capabilities, development of technical requirements, proof-of-principal development, and project management. Full development and deployment of a mobile collaborative information system for safeguards would be better left to the IAEA or a large-scale mobile platform or software vendor.

international safeguards activities, facility compliance with regulatory guidelines will be a key issue to address in order to ensure that the use of such systems are accounted for in the facility's operating license.

Keebler and Berger (2011) point out that there is "…no formal industry-wide policy for controlling the approval or use of wireless devices in [nuclear power plants]…" and so utilities are required to develop their own policies and guidelines in collaboration with national regulators, in hopes that such guidance will "…continue to mature as more emphasis was placed on this problem." Some examples of how facilities have approached the restricted implementation of wireless capabilities include a nuclear power plant that has restricted the use of cell phones in the control room, one utility that allows cell phones and portable radios from an approved vendor to use a distributed antenna system (this required utility testing of the approved models), and one utility that prohibited the use of personal cell phones inside the plant and had strict regulations regarding cell phones in approved areas.

The NRC has approached the approval of implementation of wireless networks and use of mobile devices for transmission of safeguards data on a case-by-case basis (NRC 2011-A, NRC 2011-B). The NRC does recognize the need for vigilance with such systems, and requires its licensees to submit cyber security plans for review and approval (10 CFR 73.54). IAEA inspectors will have to have agreement with operators regarding how they collect and process operator data and safeguards information onto their mobile devices if it differs significantly from current IAEA practices.

5.7.1 Regulatory Compliance and Facility Policy Mitigation Strategies

Any introduction of new technology at a facility will require negotiation with the operator, and may depend on how the facility attachments were written. Most facility attachments give leeway for new technologies and tend to specify the purpose of the equipment or measurements, rather than specify the exact piece of equipment that will be used. Allowances for remote monitoring are now also being included in facility attachments, which should make provisions for remote transmission of data. In IAEA Policy Paper 16 (IAEA 2003, SMR 2.16), Member States have agreed that remote monitoring is an acceptable means to reduce IAEA inspection efforts in facilities—if the transmission of data via a tablet could be considered under remote monitoring agreements, there is already a policy in place to support that.

5.8 Staffing

Staffing issues at the IAEA can cause delays in any technology development or deployment project because of frequent turnover of key members of technology projects. Staff rotations can result in changing technical requirements, which cause delays. Staff rotations could also lead to loss of momentum or loss of interest in a technology. In addition, an information technology project such as the deployment of a mobile collaborative information platform for safeguards would require buy-in from stakeholders across the Department of Safeguards including the Divisions of Operations, SGTS, and SGIS.

Furthermore, there is some discussion surrounding whether the IAEA will develop a mobile collaborative information platform in-house, or through a commercial vendor. For in-house development, the IAEA currently does not have sufficient staffing to accommodate a large application development project. Furthermore, because laptops are already in-use at the IAEA and have not required significant software modifications for use with IAEA safeguards, the staffing barrier will be more significant for a

mobile collaborative information platform deployment if an Android or Apple platform is selected (a Windows Pro platform would not require significant software modifications).

5.8.1 Staffing Mitigation Strategies

The staffing issue stems from the IAEA's mandatory rotation policy, as well as their zero real growth budget. Given that the IAEA does not have the capacity in-house to efficiently revamp its software for a new platform, this could be an opportunity to work with an external organization to redesign more holistically. Namely, IAEA could use an organization with software development expertise to integrate the functionality of the other safeguards inspection software used on laptops into a unified software system on a tablet. This would allow it to take a larger step forward in addressing its aging IT infrastructure as it looks to fully realize information-driven safeguards. However, this would likely be very difficult to do with software produced by the DOE national laboratories or other companies highly specialized in the nuclear field.

Gaining broad buy-in for a project across SGIS, SGTS, and the Operations Divisions may offer additional resiliency to frequent staff changes. One mechanism to support such buy-in would be to form multi-Division collaborative teams, and to tie new projects to existing IAEA efforts. For example, a new mobile platform project for the IAEA would likely benefit from working closely with the FAR team. In addition, a spiral development cycle with short development periods could serve as a more flexible approach than serial development. Spiral development can accommodate potentially changing interests or ideas as new staff join a safeguards project (Koskelo et al. 2012).

5.9 Software Transitions and Deployment

Some of the IAEA's software systems supporting safeguards verification are dated and do not translate well to mobile devices. Software designed for a laptop or desktop architecture (both hardware- and software-wise) is unlikely to easily transition to a mobile device with a completely different hardware and software architecture. In order for tablets or other mobile devices to replace laptops, all of the software that inspectors need would have to be moved from their current systems to a mobile device. Initial attempts at doing this within the IAEA have been difficult. Because the IAEA's resources are so constrained, the transition would likely need to be accomplished without significant efforts to rewrite legacy software packages.

There may also be platform-specific barriers if software is going to be deployed directly to the device. For example, Apple tightly controls the ecosystem of hardware, software, and services of iOS-based devices. If the IAEA based its mobile platform on this type of device, they would likely be required to work directly with Apple to ensure the needed application(s) could be developed and deployed.

5.9.1 Software Transitions and Deployment Mitigation Strategies

One potential mechanism to resolve software transition challenges for mobile devices would be to deploy devices running the full version of the Windows operating system (Windows "Pro" tablets). While most software would require re-engineering to run effectively on major mobile device platforms like Apple and Android, software installed on Windows "Pro" tablets can be deployed the same as it would be on any other Windows device, such as a laptop or desktop computer.

Developing web-based platforms for IAEA safeguards is another means to cope with software transition challenges, as is currently being done with the FAR project. Use of a web-based architecture would allow the IAEA to have device independence (a web page may be accessed the same way from an Apple, Android, or Windows device).This makes the solution device-agnostic as it is accessible on any device that supports a browser capable of accessing the interface. An application designed and installed on a device itself could fully function without an Internet connection, caching data offline for later upload. While web-based interfaces may be ideal for simple form entry applications such as the one being developed in FAR, more complex systems such as the Radiation Review software developed by Los Alamos National Laboratory would be very difficult to write to a web-based interface. Though developing with this paradigm may insulate a tablet project from falling prey to device changes that would require different software to be built, the specialized skill set needed for web-based development of the more complex and customized software in use at the IAEA may be a limiting factor in the use of web-based approaches.

5.10 Transparency

Transparency refers to an inspector's ability to assure an operator that only the agreed-upon capabilities of a tablet or other mobile device are being used, and that the agreed-upon data collection methods are being followed. For example, in most nuclear facilities, cameras are not allowed. While it is fairly obvious if someone is taking a photograph with a laptop, this is much harder to verify on a tablet. Tablets are commonly equipped with both a front- and rear-facing camera and it is difficult for another individual to distinguish the actions a user is taking on a tablet just by observing the user. Therefore, it may be more difficult to convince a facility operator that an inspector, while in the course of using the tablet to carry out the inspection, is not surreptitiously taking photographs.

Another transparency concern is the location and reviewability of data taken from a facility. Photos taken on a digital camera are easy to locate and review for approval with an operator directly on the device. Indeed, this is the current practice for image data. However, if images are captured and integrated with functionality within a larger safeguards application on a tablet, it may be more difficult to both locate all of the pictures for unified review and to provide assurances that these were the only photos captured.

The use of Global Positioning System (GPS) technology as part of IAEA safeguards activities is a relatively recent development that can provide inspectors with additional information regarding the size and position of objects, facilities, and sites. While geo-location information is being used in Complementary Access and in some cases for design information verification (DIV), this is still limited in practice and highly contentious among some operators. The GPS capabilities on a tablet may cause transparency issues between the IAEA inspectors and the facility operators because, as with cameras, it is not clearly observable when GPS is being used.

Furthermore, in some facilities certain data are not permitted to leave the site. Thus, if a mobile information platform is being used to operate detectors and analyze spectra, for example, the information would have to be verifiably purged from the system before the inspector leaves.

5.10.1 Transparency Mitigation Strategies

Transparency issues of mobile information platforms could be addressed partially with physical additions to a tablet. Namely, a case could be designed (or purchased if already commercially available) that physically covered the cameras on the device. This would prevent the user from capturing any photos without visibly removing the case. These cases could be inspected by the site official to provided added confirmation of their blocking capability. A specialized case with a Faraday shield could similarly prevent the user from acquiring GPS satellites without operator knowledge and consent.

Design of software can also aid in transparency. Given the acceptability of stepping through a digital camera "roll" to verify what pictures were captured, designers of a collaborative information application can implement an equivalent functionality. Regardless of how images are integrated into the data and functionality of the application for inspection and analysis purposes, all images can also be stored in a central "gallery"—as they currently are in most mobile devices. This would provide additional assurance to the site operator as he or she could see the entire collection of images in the same location. If an inspector were to go to multiple sites without syncing to headquarters, consideration would have to be given to prevent one facility operator from seeing images from another facility, perhaps via a photo gallery that is partitioned by site rather than a continuous roll.

Finally, the current approach being used in sensitive facilities to cryptographically sign all the data and allow the host to review it before it is transmitted outside the facility could also be employed for mobile information platforms.

5.11 Usability

Usability refers to the ease with which an inspector unfamiliar with a system learns its operations. This includes the ability of an individual unfamiliar with a system to use it with little or no training, and the ability for an inspector to manipulate the systems in the environments in which he will be working. While usability training is conducted for IAEA safeguards equipment and software, a mobile device may pose additional usability challenges over laptops due to potentially unfamiliar interface of a touch-screen.

A mobile collaborative information platform would require usability research in order to assess the usefulness of the systems for IAEA safeguards inspectors. Usability concerns raised during expert interviews related to the diverse technology backgrounds and languages among inspectors, as well as cultural issues that may affect the understanding of icons and buttons. Consideration must also be made for the capability to use a mobile platform in the various work situations in which an inspector will find himself. Key concerns discussed in the expert workshop included how users would interact with the device while wearing personal protective equipment and the ramifications of accidental touch when conducting an inspection on a touch-based application. How interactions with the device will be carried out if the device itself must be covered in protective equipment must also be considered. See Section 5.1.2 of this report for additional considerations of personnel protective equipment and device usability.

5.11.1 Usability Mitigation Strategies

While usability will be an important aspect of any mobile device development and deployment project, usability issues are well-understood within the information and communication technology

community. Usability lessons should be taken from other fields in which users are working in potentially dangerous or contaminated environments, such as first responders, research laboratories, or the nuclear energy industry.

The use of existing platforms with which users are already familiar and the use of homogenous user interface across functionality should decrease required training for new functionality and help inspectors become familiar with system components more quickly (Muller et al. 1990, Koskelo and Kadner 2011).

5.12 Sociocultural

Sociocultural barriers refer to implementation difficulties that arise because of differences in organizational or country-level factors based on social and cultural norms. The sociocultural barriers to IAEA deployment of tablets are several-fold. First is the IAEA's perceived risk aversion and lack of motivation to try new technologies. The IAEA is known for being hesitant to change, so developers historically have tried to use technology that is similar to that which is already in use by the IAEA, or that operates in the same way. Another IAEA-specific barrier noted in one expert interview is the general lack of urgency with respect to a need to transition to new technology. He said, "We are in the laptop era," and current technology is considered "good enough" to get the job done. Therefore, other concerns take priority and adoption of new technology is likely to be slow.

There may also be country- or facility-specific cultural barriers to technology use. For example, one former inspector noted that in the past, some countries had strict rules about importing electronic equipment into their country in order to protect the country's own burgeoning IT industry. Several interviewees noted that cooperativeness with IAEA inspectors wanting to bring in new technologies was part of the safeguards culture, and could be indicative of the greater cooperation of the State with the IAEA in general. For example, one country with a highly regarded safeguards culture required only a brief inspection of the equipment, or a verbal confirmation from inspectors regarding the intended use of the equipment.

5.12.1 Sociocultural Mitigation Strategies

Sociocultural barriers to technology deployment are persistent across technologies. However, keeping in mind sociocultural differences during technology development projects will allow staff to work with these differences, and accommodate them whenever possible. A major component of sociocultural differences is awareness and communication. Personnel working on a collaborative mobile information platform for IAEA safeguards should have training in intercultural communication, and be briefed on the institutional culture of the IAEA Department of Safeguards and its various stakeholders in a collaborative mobile information platform project.

6.0 Recommendations

In many international forums, tablets are on their way to replacing laptops. This may include the future adoption of tablets by the IAEA, accompanied by collaborative mobile information platforms. While there are barriers to deploying such platforms for international safeguards, many of those barriers are duplicative of challenges the IAEA is already addressing with the use of inspector laptops. Even for those challenges unique to tablets or other mobile technology-based systems, they do not appear to be prohibitive to the deployment of such systems. Thus, the authors conclude that the deployment of a mobile collaborative information platform for IAEA safeguards is feasible, and propose the following considerations for an IAEA mobile collaborative information platform deployment campaign:

- **Consider flexibility and ease of deployment.** New safeguards software should be developed to be useable on a tablet or laptop so that inspectors at facilities that will simply not allow tablets can still perform their critical functions within the information system. The use of web-based applications can support platform agnosticism for software with simple functionality such as form completion. The use of Windows Pro tablets may also be a solution, especially in light of obstacles in re-engineering highly customized scientific software produced by U.S. national laboratories and other scientific organizations.
- **Plan a Phased Roll-Out.** A phased roll-out of a mobile collaborative information system refers to the implementation of such a system for lower barrier-to-entry safeguards activities first, followed by a second phase to complete the deployment. The phased approach is driven by the concept that not all safeguards inspections will require the same software. Some activities, such as Complementary Access, technical visits, or safeguards inspections of facilities with limited nuclear material will likely have fewer software needs and could move to a mobile safeguards information system fairly quickly. A tablet-based system could be especially useful for Complementary Access because it could reduce the need for a camera, microphone, and GPS, and would allow inspectors to annotate photos on-site. Consolidation of such capabilities within a single device should facilitate adoption of mobile devices by inspectors for their safeguards use, and provide an introduction of the technology to inspectors before implementing them for broader use.
- **Segregate Personal and Professional Accounts.** For security purposes, it would be necessary to create a wall between professional and personal use accounts on safeguards tablets, as is currently done for inspector laptops. By allowing users to access personal accounts, this eliminates the needs to carry additional technology into the field. The separation of accounts is a commercially available capability, and does not need to be developed internally.
- **Leverage Existing Projects and Policies.** Development of mobile collaborative information platforms should tie in to current activities to limit cost and policy restrictions, and also to ensure buy-in from IAEA over the longer term. These on-going activities include remote monitoring activities (to overcome the "policy" side issues of data transmission), and the development of the new FAR software (to address staffing issues and technology acceptance).[1]
- **Consider the Spectrum of Deployment Scenarios, Costs, and Benefits.** If the IAEA does decide to adopt a mobile collaborative information platform, the potential deployment scenarios of that system

[1] This recommendation also applies to the development of PIE-IS. The development of that system should be completed with close coordination with the IAEA or other potential user groups, to ensure that the capabilities under development will meet a need within that organization and integrate with existing technologies and systems.

could vary significantly. On one end of the spectrum, an information system could be used simply as a replacement for the inspector laptop. In that scenario, inspectors would use a mobile device such as a tablet to complete paper work, interact with radiation detection equipment, monitor email, etc. However, the potential for mobile collaborative information platforms for use in international safeguards goes far beyond replacing a laptop. Mobile collaborative information platforms could enhance inspector situational awareness through real-time information updates, geo-spatial orientation and activity tracking, augmented reality, or many other capabilities. In order to better understand the gamut of potential IAEA deployment scenarios for mobile collaborative information platforms, a study should be conducted to illustrate several potential IAEA deployment scenarios for collaborative mobile information platforms, accompanied by a cost-benefit analysis of each to compare the potential safeguards effectiveness and efficiency gains to the cost of development and other deployment challenges. PNNL has been funded by NGSI to conduct such a study as follow-on research to this project in FY 2015.

Further discussions are necessary to determine the appropriate channels by which to communicate these recommendations to the IAEA.

7.0 References

10 CFR 73.54. 2014. "Protection of Digital Computer and Communication Systems and Networks." U.S. Nuclear Regulatory Commission.

Canberra. 2014. "Falcon 500® Portable HPGe-Based Radionuclide Identifier." Available at http://www.canberra.com/products/hp_radioprotection/falcon-5000.asp

Farris RK and H Medema. 2012. *Guidance for Deployment of Mobile Technologies for Nuclear Power Plant Field Workers.* INL/EXT-12-27094, Idaho National Laboratory, Idaho Falls, Idaho.

Gastelum ZN, MJ Henry, RR LaMothe, JL Barr, ER Burtner, and LE Smith. 2014. "A Safeguards Information Environment for Inspectors: Possibilities and Proof-of-Concept," PNNL-SA-100128. Presented at the IAEA's Workshop on Scanning the Horizon: Novel Techniques and Methods for Safeguards, January 2014, Vienna, Austria.

Gayne, Eva. 2010. "Information-Driven Safeguards: A country officer perspective." Presented at the 2010 Safeguards Symposium, Vienna, Austria. November 2010. IAEA-CN-184/41. Available at http://www.iaea.org/safeguards/Symposium/2010/Documents/PapersRepository/041.pdf.

IAEA – International Atomic Energy Agency. 2002. *New Safeguards Equipment Systems: Teaming IAEA Inspectors with Technology*. Department of Safeguards, International Atomic Energy Agency, Vienna, Austria. Available at http://www.iaea.org/Publications/Booklets/TeamingInspectors/teaming_inspectors.pdf

IAEA – International Atomic Energy Agency. 2003. *Safeguards Manual.* Issued October 01, 2003.

IAEA – International Atomic Energy Agency. 2004. "Procedure: Authorization of Instruments for Inspection Use." SGTS-P01/Rev.9-2004. International Atomic Energy Agency, Vienna, Austria.

IAEA – International Atomic Energy Agency. 2011. "Workshop on Sealing, Containment, and Authentication Technologies: Announcement Annex (General Technical Requirements)." Available at http://www-pub.iaea.org/MTCD/Meetings/PDFplus/2011/43123/43123_AnnexLeaflet.pdf

IAEA – International Atomic Energy Agency. 2012. *Safety of Nuclear Power Plants: Design*. Specific Safety Requirements No. SSR-2/1. Available at http://www-pub.iaea.org/MTCD/publications/PDF/Pub1534_web.pdf

IAEA- International Atomic Energy Agency. 2013., *IAEA Department of Safeguards Long Term R&D Plan, 2012-2023.* Vienna, Austria. Available at http://www.iaea.org/safeguards/documents/STR_375_--_IAEA_Department_of_Safeguards_Long-Term_R&D_Plan_2012-2023.pdf

Keebler P and S Berger. 2011. "Managing the Use of Wireless Devices in Nuclear Power Plants." *In Compliance Magazine*, November 1, 2011. Accessed March 28, 2014 at http://www.incompliancemag.com/index.php?option=com_content&view=article&id=855:managing-the-use-of-wireless-devices-in-nuclear-power-plants&catid=26:design&Itemid=130.

Korn, Chr., 1999. "Common Qualification Test Criteria for New Safeguards Equipment." IAEA Technical Note I.99.105, April 1999.

Koskelo M and S Kadner. 2011. "Safeguards Instrument Sustainability: A Paradigm Shift." In *52nd Annual Meeting of the Institute of Nuclear Materials Management 2011 (INMM 52).* Curran Associates, Red Hook, New York.

Koskelo M, H Undem, M Good, S Frazar, M Schanfein, and S Kadner. 2012. "Spiral Development for Safeguards Instrumentation." In *53rd Annual Meeting of the Institute of Nuclear Materials Management 2012. (INMM 53).* Curran Associates, Red Hook, New York.

Muller R, OJ Heinonen, and D Schriefer. 1990. "IFSS: The IAEA's inspection field support system, A description of computer support to safeguards inspectors." *IAEA Bulletin*, 1/1990. Available at http://www.iaea.org/Publications/Magazines/Bulletin/Bull321/32103452730.pdf.

Novatchev D, P Titov, B Siradjov, I Vlad, and X Wang. 2010. "In-Field Inspection Support Software: A Status Report on the Common Inspection On-site Software Package (CIOSP) Project." In *Proceedings of Symposium on International Safeguards Verification and Nuclear Material Security 29 October – 2 November 2001, Vienna,* IAEA-SM-367/13/03. Available at http://www-pub.iaea.org/MTCD/publications/PDF/ss-2001/PDF%20files/Session%2013/Paper%2013-03.pdf.

NRC. 2011."Response to South Texas Project (STP) with Approval to Use Mobile Telephone Devices for Electric Transmission of Safeguards Information (SGI). November 9, 2011. Available at http://pbadupws.nrc.gov/docs/ML1130/ML113050166.html

NRC. 2011. "Use of Mobile telephone Devices for Electronic Transmission of Safeguards Information." Letter to Mr. Douglas R. Bauder, October 4, 2011. Available at http://pbadupws.nrc.gov/docs/ML1127/ML112730196.pdf

Peixoto, OJM, HL Gonzales, E Palacios, JY Lefebvre. 2001. "Coordination Improvement on Safeguards Application Between ABACC and IAEA." In *Proceedings of Symposium on International Safeguards Verification and Nuclear Material Security 29 October – 2 November 2001, Vienna,* IAEA-SM-367/12/07. Available at http://www-pub.iaea.org/MTCD/publications/PDF/ss-2001/PDF%20files/Session%2012/Paper%2012-07.pdf

Penny Stocks Lab. 2014. "Infographic: The Golden Age of Mobile." Accessed July 20, 2014 at http://pennystocks.la/blog/golden-age-of-mobile.

Petersen S, P Doyle, S Vatland, C Salbu Aasland, TM Andersenm, and D Sjong. 2007. "Requirements, Drivers and Analysis of Wireless Sensor Network Solutions in the Oil and Gas Industry." 12th IEEE International Conference on Emerging Technologies and Factory Automation. September 25-28 2007, Patras, Greece.

St. Pierre, DE, KL Steinmaus, and BD Moon. 1994. "International Nuclear Safeguards Inspection Support Tool (INSIST)." In *35th Annual Meeting of the Institute of Nuclear Materials Management (INMM 35).* Curran Associates, Red Hook, New York.

Appendix A

IAEA Technology Adoption Process

Appendix A

IAEA Technology Adoption Process

The International Atomic Energy Agency (IAEA) often relies upon Member State support programs (MSSPs) and commercial off-the-shelf (COTS) equipment providers for development of safeguards equipment as the IAEA does not have the means to maintain a large research, development, and production capability. However, the evaluation of equipment for use as part of verification activities is largely the responsibility of the IAEA with some reliance on MSSPs for field testing. The final authorization to use equipment for inspection activities rests solely with the IAEA. Any technology to be used by safeguards inspectors, therefore, would go through the IAEA's technology adoption process (IAEA 2004).

The request to develop, authorize, or modify equipment or software for use by IAEA inspector as part of their verification activities comes from either the Department of Safeguards Division of Technical Support (SGTS) or one of the Operations Divisions. When the request is made, an analysis of alternative technical solutions is performed. This analysis is then passed to the IAEA's Equipment Coordination Committee (ECC), a group comprised representatives from multiple departments responsible for "the approval of development and evaluation tasks and the authorization of new instruments for inspection use." In order to review a piece of equipment, the ECC must receive documentation of user requirements containing information on

- system functions
- system performance
- non-functional considerations including authentication and usability requirements
- required calibrations and maintenance
- required documentation
- necessary training for Division of Operations and SGTS
- facility details and constraints for equipment with facility specific applications.

Once a piece of equipment has been approved for development by the ECC, it is considered "under development" and classified as Category C equipment. Before the ECC can approve a piece of equipment to enter Category B, the evaluation phase, a final development report must be written. The report includes a final design report confirming needs identified in initial request have been met, the equipment configuration, manufacturer, software, and technical specifications. Additionally, an evaluation plan must be written that defines the exact parameters under which the equipment will be tested under the evaluation phase such as:

- acceptance tests against previously defined requirements
- necessary laboratory tests
- environmental tests

- usability tests
- vulnerability review (if required, a third-party vulnerability assessment is performed[1])
- required field tests and initial safety evaluation.

Should the ECC approve the equipment for evaluation, the equipment enters Category B, known as "under evaluation." During evaluation, operating, inspection, and maintenance procedures are developed for the equipment. Testing, as defined in the evaluation plan, is completed. Some equipment may then move to a subcategory, Category BD. Equipment enters this subcategory as a part of field testing if data collected by the instrument during testing can be used for inspection purposes. Not all equipment in Category B will reside in Category BD, only equipment approved by the ECC for use under strictly defined conditions at specified facilities. Equipment can reside in Category BD for 12-24 months, with a review and approval required for continued use after 24 months.

Once all tests have been completed, a final evaluation report that documents the results of testing and provides all documentation for operation, training, implementation, safety, and maintenance is prepared and submitted to the ECC. If recommended for inspector use by the ECC and authorized by the director of SGTS the equipment enters Category A, "authorized for inspection use," and can be used by inspectors for verification activities. Modification to authorized equipment can be made with review by the responsible section head within SGTS. However, some modifications may require reevaluation (as defined by the plan developed for evaluation phase) and ECC approval prior to deployment. Updates to previously authorized instrumentation software must be reevaluated "using criteria specified in the Procedure for Authorization of Equipment Systems and Instrumentation Software (only available from SGTS Director's Office)." Once that testing has been completed the software can be "made available for routine use." (IAEA 2003, section 4.4.2.2)

While equipment developed by the IAEA or MSSPs follow this procedure, some equipment, such as joint-use instruments or commercially available equipment, are typically immediately accepted into Category B. For this case, a set of common qualification test criteria has been developed by the IAEA and EURATOM (Korn 1999).[2] The criteria are

- an operational test (operation in standard configuration and expected environment for extended time period)
- thermal and humidity tests (testing of temperature limits, and humidity limits under varying temperatures)
- mechanical tests (vibration testing, drop and shock testing)
- electromagnetic tests (voltage stability, emissions).

Additional testing can be added to the development and adoption process for new equipment. This has been demonstrated during development of the IAEA's Next Generation Surveillance System (NGSS) being developed by the U.S. and German support programs to the IAEA. Irradiation testing was

[1] Per the IAEA's "Authorization of Instruments for Inspection Use," (IAEA, 2004) a third party vulnerability assessment is required for new systems that incorporate cryptography for data authentication, communications, or encryption of sensitive data.

[2] The IAEA and ABACC also have a specific procedure and qualification criteria for the joint-use of safeguards equipment. However, this information is considered sensitive and not publicly available. See Peixoto et al.

performed to determine the reliability of the system under exposure to gamma rays and thermal and fast neutrons. Also, a mean-time between failure (MTBF) test will be performed using initial field deployed units and software to identify the theoretical MTBF.

Appendix B

Expert Sources

Appendix B

Expert Sources

Expert Sources interviewed and included in the expert workshop are listed below.

Shirley Johnson, IAEA (retired)

Keith Tolk*, Sandia National Laboratories (retired)

Chris Dalton*, Malorkus Worldwide LLC

Mike White, Aquila Technologies

Michael Henry, Pacific Northwest National Laboratory

Russ Burtner, Pacific Northwest National Laboratory

Cal Delegard*, Pacific Northwest National Laboratory (retired)

Ben McDonald, Pacific Northwest National Laboratory

Dick Kouzes, Pacific Northwest National Laboratory

Eric Smith*, Pacific Northwest National Laboratory

Halvor Undem*, Pacific Northwest National Laboratory (retired)

Jacob Benz, Pacific Northwest National Laboratory

Jonathan Barr, Pacific Northwest National Laboratory

Mario Fernandez, Nuclear Regulatory Commission

Helly Diaz Marcano*, of Savannah River National Laboratory

*Participants also have IAEA experience.

Pacific Northwest
NATIONAL LABORATORY

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

U.S. DEPARTMENT OF
ENERGY

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

www.pnnl.gov