# SANDIA REPORT

SAND2014-18291
Unlimited Release
Printed September 2014

# The Feasibility of Mobile Computing for On-Site Inspection

Karl E. Horak, Sharon M. DeLand, and Dianna S. Blair

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.



Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.



Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-2087
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: http://www.ntis.gov/help/ordermethods.aspx#online

SAND2014-18291
Unlimited Release
Printed September 2014

# The Feasibility of Mobile Computing for On-Site Inspection

Karl E. Horak, Sharon M. DeLand, and Dianna S. Blair
International Safeguards & Technical Systems (06832)
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1371

**Abstract**

With over 5 billion cellphones in a world of 7 billion inhabitants, mobile phones are the most quickly adopted consumer technology in the history of the world. Miniaturized, power-efficient sensors, especially video-capable cameras, are becoming extremely widespread, especially when one factors in wearable technology like Apple's Pebble, GoPro video systems, Google Glass, and lifeloggers. Tablet computers are becoming more common, lighter weight, and power-efficient. In this report the authors explore recent developments in mobile computing and their potential application to on-site inspection for arms control verification and treaty compliance determination. We examine how such technology can effectively be applied to current and potential future inspection regimes. Use cases are given for both host-escort and inspection teams. The results of field trials and their implications for on-site inspections are discussed.

## ACKNOWLEDGMENTS

The authors would like to thank:

Andrew Steele for playing a key role in obtaining our set of Google Glass; Joe Lewis for an important early draft review; Dan Wurmser, Larry Denyer, Don Clagett, and Mark Lavens for insightful comments, document review, and valuable information based on their OSI experience; and Anne Choi for project oversight, document review, and connecting us with State Department subject matter experts.

# CONTENTS


1. Executive Summary ..... 9

2. Introduction ..... 11
- 2.1 On-Site Inspection ..... 12
- 2.2 Mobile Computing Capabilities ..... 12
- 2.3 Existing OSI Equipment for Compliance Monitoring ..... 13

3. POTENTIAL USES OF MOBILE DEVICES DURING OSI ..... 15
- 3.1 A Compendium of Tasks and Activities ..... 15
- 3.2 Use case #1—Mobile Devices for Inspection Team Information Support ..... 18
- 3.3 Use case #2—Measurement and Sampling ..... 20
- 3.4 Use case #3—Managed Access ..... 20
- 3.5 Use case #4—Training ..... 21
- 3.6 Other OSI-related Uses for Mobile Computing Technology ..... 22

4. IMPEDIMENTS, RISKS, AND MITIGATIONS ..... 25
- 4.1 Inspected State Party Perspective ..... 28
- 4.2 Inspection Team Perspective ..... 28
- 4.3 Deployment Options ..... 29

5. FIELD STUDIES ..... 31
- 5.1 Proof-of-Concept Field Exercises ..... 31
  - 5.1.1 Notional Weapon Storage Scenario ..... 31
  - 5.1.2 Experimental ..... 31
  - 5.1.3 Activities ..... 31
- 5.2 Results ..... 32
  - 5.2.1 Video recording ..... 32
  - 5.2.2 Digital photography and audio notes ..... 33
  - 5.2.3 Mobile video-conferencing ..... 33
  - 5.2.4 Inspection tracking ..... 34
  - 5.2.5 QR codes ..... 34
  - 5.2.6 Managed access ..... 35
  - 5.2.7 Time to complete activities ..... 35
  - 5.2.8 Google Glass ..... 36
  - 5.2.9 Overall ..... 36
- 5.3 Additional Proof-of-Concept Exercises ..... 37
  - 5.3.1 Augmented Reality Applications ..... 37
  - 5.3.2 Integrated Security Facility ..... 39

6. ARE MOBILE TECHNOLOGIES FEASIBLE FOR OSI? ..... 41
- 6.1 Feasibility for CTBT ..... 41
- 6.2 Feasibility for FMCT ..... 42
- 6.3 Feasibility for CWC Challenge Inspections ..... 43
- 6.4 Feasibility for Strengthened Safeguards ..... 44
- 6.5 Overall Conclusions ..... 44
  - 6.5.1 Feasibility for Future Treaties ..... 44

7. RESEARCH OPPORTUNITIES AND NEXT STEPS ..... 47
8. REFERENCES ..... 49
9. APPENDIX A ..... 51
10. APPENDIX B ..... 53
11. APPENDIX C ..... 55
Distribution ..... 56

## FIGURES

Figure 1 Side by side comparison of a 1989 laptop with a current tablet computer ..... 11
Figure 2 The inspection facility used for the exercise and our videographer ..... 33
Figure 3 Interior view of Bunker 8013 showing north (left) and south sections ..... 33
Figure 4 Sample output from a COTS GPS tracking app ..... 34
Figure 5 Screen capture of QR code-based inventory app ..... 35
Figure 6 Mock undeclared items ..... 35
Figure 7 General view of inspection area ..... 35
Figure 8 Using a GPS app ..... 36
Figure 9 Taking a radiation measurement ..... 36
Figure 10 Screen capture of an AR app identifying a building ..... 37
Figure 11 A virtually shrouded item as seen with a smartphone app ..... 38
Figure 12 Glove boxes, overhead piping, and gantry crane ..... 40
Figure 13 Hot cells with manipulator ..... 40
Figure 14 Material storage area ..... 40
Figure 15 Communications and security features visible during walk-through ..... 40

## TABLES

Table 1 Potential Uses of Mobile Devices and Apps ..... 15
Table 2 Risks, Consequences, and Mitigations ..... 26
Table 3 Summary of Scenarios and Activities (S1-S7) ..... 32
Table 4 Elapsed Time for Activities ..... 36
Table 5 Dimensions (cm) of Selected Items of Concern ..... 39
Table 6 Summary of Mobile Functionality and Possible Limitations ..... 41
Table 7 Potential Research Topics and Follow-on Activities ..... 47
Table 8 Equipment for Selected Treaties ..... 51

# NOMENCLATURE

| | |
|---|---|
| AP | Additional Protocol |
| App | Short for “application,” usually referring to software on a mobile device |
| AR | Augmented Reality |
| BWC | Biological Weapons Convention (Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction) |
| CDMA | Code Division Multiple Access |
| CFE | Treaty on Conventional Forces in Europe |
| COTS | Commercial Off-the-shelf |
| CTBT | Comprehensive Nuclear Test-Ban Treaty |
| CTBTO | Comprehensive Nuclear Test-Ban Treaty Organization |
| CWC | Chemical Weapons Convention (Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction) |
| DIV | Design Information Verification |
| DOD | Department of Defense |
| DTRA | Defense Threat Reduction Agency |
| FMCT | Fissile Material Cutoff Treaty |
| GIS | Geographical Information System |
| GPS | Global Positioning System |
| GSM | Global System for Mobile Communications |
| HDMI | High Definition Multimedia Interface |
| IAEA | International Atomic Energy Organization |
| ID | Identification |
| INF | Intermediate-Range Nuclear Forces Treaty |
| ISF | Integrated Security Facility |
| ITC | International Training Course |
| KAFB | Kirtland Air Force Base |
| LED | Light Emitting Diode |
| MDM | Mobile Device Management |
| NFC | Near-Field Communications |

| | |
|---|---|
| NPT | Non-Proliferation Treaty (Treaty on the Non-Proliferation of Nuclear Weapons) |
| NSCOE | Nuclear Security Center of Excellence |
| NWS | Nuclear Weapon State |
| OPCW | Organisation for the Prohibition of Chemical Weapons |
| OSI | On-Site Inspection |
| OSIS | On-Site Inspection System |
| PIDAS | Perimeter Intrusion Detection and Assessment System |
| PNET | Peaceful Nuclear Explosions Treaty |
| POE | Point of Entry |
| QR | Quick Response |
| RFID | Radio Frequency Identification Device |
| SD | Secure Digital |
| SIM | Subscriber Identity Module |
| SMS | Short Message Service |
| SNL | Sandia National Laboratories |
| SSH | Secure Shell (a cryptographic Internet protocol) |
| SSL | Secure Socket Layer |
| SUI | Sensitive User Information |
| START | Strategic Arms Reduction Treaty |
| TRIS | Trusted Information System |
| TTBT | Threshold Test Ban Treaty (Treaty on the Limitation of Underground Nuclear Weapon Tests) |
| UML | Unified Modeling Language |
| UN | United Nations |
| UN Convention | United Nations Convention Against Traffic in Narcotic Drugs and Psychotropic Substances |
| URL | Uniform Resource Locator |
| USB | Universal Serial Bus |
| Wi-Fi | Wireless local area network (a play on the term “Hi-Fi” for high fidelity) |
| WLAN | Wireless Local Area Network |

# 1. EXECUTIVE SUMMARY

On-site inspection (OSI) is a valuable verification tool and confidence-building measure for international treaties and agreements. With the increasing availability of commercial mobile and wearable computers, inspection-relevant data can be collected and retrieved on site using a variety of sensor systems, data management tools, and information systems. Recent advances in mobile computing capabilities, including smartphones and tablet computers with cellular/wireless networking capability, advanced audio-video recording features, global positioning systems, and other on-board sensors represent opportunities to provide both inspected state parties (host and/or escorts) and inspection team members with convenient access to information and efficient data recording tools.

Potential uses focus on information management and include audio, video and photographic recording, inspection team tracking and other GIS applications, enhanced communications, real-time information access, situationally-aware information feeds, and sensor monitoring. While these capabilities offer increases in efficiency and effectiveness, they also present challenges. Protecting sensitive information, equipment, and material while smartphones and tablet computers are in use nearby requires careful attention to risks and their mitigations. Authenticated dual access to shared information may be required. The simplest solution is to restrict smartphones and tablets to the inspected state party only. This will certainly expedite escort duties, but it will not substantially help the inspectors except indirectly.

This report explores four use cases for mobile technologies: inspection team information support, measuring and sampling, managed access, and training. The report also considers their uses and provides the results from proof-of-concept field exercises.

The feasibility of mobile device use during OSI hinges on the risk-benefit calculation of the parties involved. The effectiveness of possible mitigations must be balanced against advantages to the inspection process. These benefits may include reduced interruptions to operations, increased safety, enhanced thoroughness, more effective hosting/escorting, more rapid determination of results, and more accurate recording of activities.

By and large, any one mobile feature, for example, GPS, is available as a stand-alone, single purpose device. However, the integration of such features and communications channels within a convenient, customizable, portable package makes smartphones and tablet computers both attractive as an inspection tool and forbidding as a security risk.

Because facility owners may tightly control their personnel and highly customize their escort's mobile platforms, these technologies have a much broader application for the inspected state party. Hosts/escorts can be trained well ahead of time, equipment can be properly configured (and if necessary, features disabled), and policies for use put in place. With well-thought-out administrative and engineering controls, it is conceivable that mobile computing devices can be brought safely and securely into even sensitive areas by facility personnel.

Inspection parties wishing to use mobile computing capabilities on the other hand, must operate within the sometimes strict limitations of treaties or agreements and facility constraints. Under current OSI regimes, there are few opportunities for applying mobile computers to inspection team activities. Inspectors may find that these technologies are best applied in training and to make efficient use of time while en route to and from sites.

For agreements currently in force with rigorous equipment specifications, it seems doubtful that mobile devices will be allowed on inspection visits. That does not mean that in an offsite operations center or other location smartphones, tablets, and wearable systems will not be valuable adjuncts to the parties' information and communication systems.

However, in future treaties and agreements consideration should be given to the impact and utility of mobile internet and communications technologies. As devices become smaller and less conspicuous and they become more widespread and socially acceptable, it is possible that they will find acceptance and use for both host and inspection team OSI activities.

# 2. INTRODUCTION

On-site inspection (OSI) is a valuable verification tool and confidence-building measure for international treaties and agreements (Gough and Zelicoff 1993). With the increasing availability of commercial mobile and wearable computers, inspection-relevant data can be collected and retrieved on site using specialized data management systems.

One early example of such a system was the On-Site Inspection System (OSIS) developed at Sandia National Laboratories in the early 1990s (DeLand et al. 1996; Bray and DeLand 1997). At that time, laptop computers were relatively large, heavy, awkward to use unless seated, and had limited battery life. Figure 1 below shows the dramatic reduction in size that has occurred in the last 25 years.

**Figure 1 Side by side comparison of a 1989 laptop with a current tablet computer.**

The current generation of mobile devices range from hand-carried smartphones and lightweight tablets to wearable devices such as Google Glass, Zypad (wrist-wearable computer), lifelogging devices (webcams worn as a necklace, on the lapel, or as headgear), and even virtual retinal displays (Wearable Computer - Wikipedia 2013). With the rate of technological change, one can reasonably expect mobile computers to continue to be reduced in size, diminished in weight, enhanced in usability, extended in capability, and increased in battery life.

Form factors will evolve significantly over time, but for our purposes in this paper we wish to explore if mobile computing as it exists at the present time or near-term foreseeable future can be applied to OSI. If its use is feasible for OSI, how can such technology be effectively applied to inspection regimes?

## 2.1 On-Site Inspection

For the purposes of this feasibility study, we are concerned with all aspects of OSI from inspector and escort training through actual inspection activities to post-inspection analyses. Arms control inspections usually have several key activities (DTIRP 3008):

- Inspection notification;
- Pre-inspection planning;
- Travel logistics;
- Pre-inspection briefing;
- Inspection;
- Post-inspection briefing; and
- Inspection report writing and submission.

Inspection activities may include:

- Access to specified facilities and infrastructure;
- Taking photographs (if permitted under the treaty or agreement) using still cameras, video cameras, and possibly aerial photography;
- Conducting interviews, usually of facility personnel (past and present);
- Sampling of items which may include ground, air, water, or biomedical samples; and
- Review of document and records.

To protect sensitive information, arms control inspections are limited to collecting only the information required to verify compliance. However, in the event the Inspected State Party declines to provide the requested information, some treaties allow the Inspected State Party to show compliance through alternate means (typically negotiated with the inspection team). Treaties or agreements with these sorts of provisions are said to be practicing "managed access."

## 2.2 Mobile Computing Capabilities

Modern mobile devices such as smartphones and tablet computers can vary widely in capabilities, but generally have a fairly common core set of features:

- Display
- Speaker and/or audio jack
- Microphone
- CPU
- Battery
- Wireless communication (NFC, Wi-Fi, Bluetooth, etc.)
- Cellular communication (GSM, CDMA)

For use as a full-featured inspection support tool, we assume here that modern, relatively complex devices are used with high-resolution touchscreens and state-of-the-art mobile operating systems. Other features that may be particularly useful in the field for either inspectors or inspected state parties include:

- Global Positioning System (GPS)
- Compass/magnetometer
- Accelerometer
- Gyroscope
- Thermometer
- Cameras (high resolution still and video)
- LED lights (camera flash, flashlight, etc.)
- Video playback and HDMI output
- Audio, light, and vibration alarms and alerts
- Ambient light sensor
- Proximity sensor
- Multitouch gesture input
- Radio receiver
- SIM card
- Personal productivity software (word processor, spreadsheet, etc.)
- Email, instant messaging, and push alerts
- Web browsers
- Wireless tethering (creating a Wi-Fi internet access point)
- Hardware connectivity and expansion (USB and/or proprietary interfaces)
- Memory card reader (SD and micro-SD)
- External keyboard support/docking stations
- Customized applications (apps)

Other capabilities are being regularly deployed by device manufacturers. For example, some mobile devices today have onboard radiation monitors, barometers, lux meters, carbon monoxide detectors, infrared thermometers, or gas leak detectors. Third-party app developers are continuously releasing ingenious programs that run on mobile devices and integrate hardware functions in novel ways. Accessory lenses are now available for iPhones. A 3-D laser scanner add-on for mapping interior spaces is about to come onto the smartphone market.

## 2.3 Existing OSI Equipment for Compliance Monitoring

Appendix A summarizes the state of affairs in general terms for OSI equipment across 13 international agreements, treaties, or draft treaties (Finno 2000). Appendix A shows that the CTBT, OPCW, INF, TTBT, and PNET each have or refer to lists of agreed-upon equipment. Most commonly these treaties allow for cameras, transmission equipment, sampling devices, and containment devices (tags and seals). Similarly, standard Safeguards inspections and Additional Protocol inspections have equipment specified in facility attachments, which are usually confidential.

Examination of the sections of the Protocol to the Comprehensive Nuclear Test-Ban Treaty related to OSI (Appendix B) shows that mobile devices may be considered appropriate, but only under restricted circumstances. Paragraph 37 of the equipment annex of the CTBT includes the phrase “auxiliary equipment for the effective and timely conduct of on-site inspections.” Paragraph 62 states, “The members of the inspection team shall have the right at all times during

the on-site inspection to communicate with each other and with the Technical Secretariat. For this purpose they may use their own duly approved and certified equipment with the consent of the Inspected State Party, to the extent that the Inspected State Party does not provide them with access to other telecommunications."

In the INF treaty's inspection protocol (U.S. State Department 1987), we find detailed specifications for allowable equipment and its use. The INF even specifies the number of phone lines to be available to the Inspection Team.

Some treaties have gone to extremes in specifying the rights of access to be accorded the personnel and equipment of the inspecting state. START, for example, specifies the maximum number of spare flashlight bulbs and the lengths of rulers that inspectors may carry (START, 1990, Annex 8, § II, ¶ B(1)).

In light of this, mobile devices may be seen as an unforeseen combination of communication device, personal assistant, GPS, camera, and video-camera. As such, they are not so much revolutionary as evolutionary – convenient combinations of commonly used (or prohibited) OSI equipment. In many treaties and agreements one finds references to "other equipment, as agreed by the Parties," which certainly would open the door for their use. The fact that mobile devices can be heavily customized and programmed makes them powerful, useful, yet awkward to control, difficult to manage, and challenging to limit in terms of functionality. Changing allowable equipment in existing OSI regimes, especially to something that is multipurpose and powerful, will be difficult.

# 3. POTENTIAL USES OF MOBILE DEVICES DURING OSI

Inspected state parties may unilaterally implement the deployment and use of such devices in facilities under their control. Inspection teams, on the other hand, must work within the limitations of the treaty or agreement that mandates their activities. Some functions of mobile devices, for example, voice telephony, could be of obvious benefit to either or both parties.

Smartphones and tablet computers bring a wide variety of information management tools to the OSI setting. Both host and inspector may profit by their use, but the host has more flexibility in that they can use site-specific pre-approved hardware systems that meet their facility's safety and security constraints. Similarly, the host is likely to create dedicated apps and webpages just for mobile host team members. It is also conceivable that the host will develop apps specifically for use by the inspection team or possibly the general public.

On the other hand, inspection teams will have requirements specific to the treaty regime in which they are operating and their mobile information systems can offer targeted solutions. However, as discussed in section 4, there may be significant challenges to overcome before an Inspected State Party will permit external mobile devices into a sensitive site.

## 3.1 A Compendium of Tasks and Activities

The more obvious technologies for use during OSI with managed access are summarized below (Horak, Bleakly, and McDaniel 2013).

**Table 1 Potential Uses of Mobile Devices and Apps**

| Purpose | Description |
|---|---|
| Inspection team tracking | Using secure types of Foursquare-like or Map My Walk-like software |
| Photography and videography | In lieu of film cameras or stand-alone digital cameras |
| Enhanced communication channels | Text messaging, microblogging, social media, image sharing, video-teleconferencing |
| GIS applications | Mapping, orientation, familiarization |
| Novel sensor packages | Either intrinsic COTS sensors or add-ons |
| Real-time information access and situationally-aware information feeds | Information available on demand/as needed |
| | Superimposing information and images upon the camera field of view |
| | Data recording and transmission based on location, activity, and context |
| Sensor monitoring | Remote real-time viewing of data and video from sensors |
| Educational Outreach | Mobile devices in use by private citizens and social media can be a channel for increasing public awareness of arms control efforts. |

Inspection team tracking could be performed automatically or with a Foursquare-like check-in procedure. At significant waypoints, the user (host or inspector) would check-in and have their GPS coordinates, time-date stamp, photographs, and comments logged onto a central system. Team tracking could be unilateral (host only or inspection team only) or bilateral (location information shared to all participants).

In lieu of stand-alone film cameras, digital cameras, and camcorders, the built-in cameras of mobile devices could be used by either or both parties. The joint use of images and video obtained during and inspection will require consideration. Issues of image authenticity, veracity, and confidentiality need to be dealt with in a secure and reliable fashion. This represents an area where further research would be of benefit. Understanding the breadth and depth of security concerns along the data pathway from verifiable code on the device to authenticated, encrypted delivery to an information consumer or secure storage is critical. Vulnerability testing, red teaming, and acceptance testing would need to be performed prior to any actual use in a verification application.

Mobile devices can provide enhanced communications due to their multi-channel capabilities—Wi-Fi (WLAN), Bluetooth, and cellular radios. While two-way radios form the backbone of current escort and inspection team communications, the ability of mobile computers to provide more than voice transmission is an important strength of theirs. One can envision e-mail, cell phone, and SMS text messaging between teams, between inspectors and escorts, and between field teams and operations center. SMS services for text messaging and microblogging (Twitter-like), social media services for sharing observations and events (Facebook-like), and image sharing services (Flickr-like) could be possible with a properly configured and secured cell phone or tablet. Video-teleconferencing may be carried out with commercial systems like Skype, Facetime, or Hangouts, although proprietary channels may be preferred.

GPS capabilities allow mobile users to accurately know their location, elevation, and orientation. IAEA and UN inspectors in Iraq in the early 1990s were sometimes misled by their minders. Stand-alone GPS units were needed to confirm inspection locations (Kay 1995). Similar tools in cell phones can track one's inspection route for later playback or analysis. Again, either the host, the inspector or both could make use of this technology (Bleakly, Horak, and McDaniel 2012).

Cell phone technology continues to draw innovation from a wide number of developers, both professional and hobbyists. Novel sensor packages appear frequently, for example, a simple radiation detector based on a cell phone camera with its lens covered ("Gamma Rays Caught on Camera" 2013) or a spectrometer made by adding a diffraction grating over the lens (Scheeline and Kelley 2013). These ad hoc and first-generation smartphone sensors lack the sensitivity to replace current professional-grade detection devices. Significant advances in capability and reductions in cost need to be made before COTS mobile devices can approach the accuracy of dedicated sensors. That said, equipment manufacturers are often including Bluetooth or Wi-Fi data outputs, which can make mobile devices a convenient data viewing and recording platform.

Where wireless service is adequately reliable, real-time database access could be provided. This might be facility-supplied local information sent to the escort team, for example, chemical hazards and safety data. Such information could be a common source for digital copies of

declarations, inspection mandates, treaty or agreement text, open-source maps and photographs, documents released by Inspected State Party to the inspection team, etc. These may be fully open to the public at large or restricted to just the parties to the inspection. The information could be from an internal database (either public or restricted) shared with the inspection team or it could be from some other source and supplied to all parties during an inspection.

We recognize that the weak link in the OSI process is the human factor. Mobile devices can help by getting routine activities done more quickly and allowing the inspector's time to be concentrated on anomalies. Many use cases can be envisioned:

- Full-text of declarations and inspection mandates, available on demand
- Online digital photography archives, diagrams, and equipment specifications
- Inspection checklists, notes, and previous inspection reports
- Inspection templates and forms for ease of data entry
- Inspection-relevant items tagged with QR codes (along with traditional tamper-indicating tags or seals) to facilitate item lookup in appropriate databases
- Site maps, satellite imagery, aerial imagery
- Virtual 3D facility models
- Online safety information
- Environmental or other wide area monitoring data

Another possibility is situationally-aware information – data that is sent to one's phone or tablet based on sensed activities. Mobile devices can "know" whether their user is moving or stationary, keying in information or browsing webpages, using the camera at a particular location facing a particular direction, and many other states, even the light level the user is experiencing.

Situationally-aware information could enable accountability during an inspection: GIS information, video and audio evidence, RFID markers, and user conformations could be used to validate presence and verification.

Mobile technologies also can enable the viewing of real-time data and video from sensor systems in the field. Cellular, Wi-Fi, Bluetooth, and NFC channels are available to communicate with various networked sensors and monitoring systems. For example, video streams during portal and perimeter monitoring of a CWC challenge inspection could be viewed by authorized personnel on their smartphones or tablets. Small, extremely portable, light weight, environmentally hardened video systems are now available (for example, the GoPro, "GoPro Official Website: The World's Most Versatile Camera" 2013). Their video feeds may be shared by Wi-Fi with appropriate viewers' mobile devices.

Mobile devices may be configured to read QR codes that store addresses and Uniform Resource Locators (URLs). Other similar industry-standard codes are also available: data matrix, Aztec code, and micro QR code. These may appear on almost any object about which users might want information. Users with a camera phone equipped with the correct reader application can scan the image of the QR code to display text, show contact information, go to a location on Google Maps, connect to a wireless network, or open a web page in the telephone's browser. QR codes also may be linked to a location to track where a code has been scanned. Either the

application that scans the QR code retrieves the geoinformation by using GPS and cell tower triangulation or the URL encoded in the QR code itself is associated with a location. QR codes can contain more information than a standard linear barcode of similar size. However, there are risks associated with QR codes. QR codes can carry executable data as JavaScript in the URL data format, but this is only executed in a regular browsing mode. This exposes systems to no more risk than opening any web page.

Augmented reality (AR) is the process of superimposing additional data upon a computerized view of a real-world scene. Commonly this is done with visual elements added to the view as seen with a smartphone's camera. Whether simple graphical elements, supplementary text, or complex multimedia presentations, the processing is done in real-time and adds to or augments one's perception of a scene (Hung-Lin, Shih-Chung, and Xiangyu 2013).

One can imagine this sort of system providing an escort with visual safety warnings or an inspector with overlaid imagery from previous visits. Recently AR has received considerable publicity with the announcement by Google of their wearable heads-up AR display, Google Glass ("Google Glass - Home" 2013).

Technology now exists that allows small, low-cost COTS aerial drones to be controlled remotely by smartphone (for example, Parrot 2013). These drones can display and capture forward and downward video. Their use in monitoring and verification inspections has not been explored here, but offer interesting options for perimeter monitoring, site familiarization, and Inspected State Party-only surveillance.

## 3.2 Use case #1—Mobile Devices for Inspection Team Information Support

Mobile devices offer a large set of useful tools for OSI in a convenient package. Smartphones, tablets, and wearable computers could be useful for many of the tasks listed in Table 1. Of direct interest to the inspection team will be a variety of communication channels, photography and videography, GIS applications for team tracking and orienting the inspectors on the ground, real-time access to information, situationally-aware information feeds, and sensor monitoring.

Within any sensitive facility or area there will likely be limitations on allowable technologies. Photography and videography are a special concern due the possibility of visually recording sensitive scenes. Also, some sites will place restrictions on transmitting devices (Bluetooth, Wi-Fi, and cellular connections). Some safety limitations have to do with contamination issues while others simply are a matter of the use of electrical devices near flammable chemicals. With proper planning plus suitable administrative and engineering controls, it may be possible to negotiate the use of these devices in particular settings. Under some OSI regimes there will be concerns about digital storage media leaving the site. On-site storage of the digital media under seal may be necessary to ensure that previous inspection images are not altered, even when the digital media must remain inside a facility.

An alternative would be to allow the host or escort personnel to control the mobile device. This would provide assurances that the apparatus is not being misused or accidentally revealing

sensitive information. This strategy, by introducing a gatekeeper, interferes with or at least delays the instantaneous and unfiltered flow of information to the inspectors. However, it may be an acceptable alternative in some circumstances. Case-by-case analysis of inspection sites, facilities, and mandates will be necessary to determine how mobile computers can be integrated, if at all, in a particular scenario.

The current generation of smartphones is capable of providing a highly portable and powerful feature set to support inspection team activities. Smartphones appear to be better suited as data delivery and data capture devices rather than data entry devices. Entering more than a few sentences of text is tedious, while reading a large document is manageable. Carefully designed templates and forms with useful pull-down menus and pre-populated values can improve the user experience and accuracy of data entry. Some data capture tasks, especially audio recording and still or video photography, are especially well suited to smartphones. Current viewscreens are susceptible to glare and sometimes difficult to use in bright sunlight.

Smartphone browsers are entirely capable of producing readable results from online database queries and searches. Proper use of responsive design is important to enhance readability on small screens. Customized apps could provide an even higher level of user experience, including cached data sets for use when phone or network connectivity is lost.

Tablet computers offer many of the same features as smartphones, but with increased dimensions: larger screen, longer battery life, more memory. That, of course, comes at a cost of increased size and weight.

With a larger screen, data entry becomes easier due to the increased legibility and increased size of the virtual keyboard. External keyboards greatly improve typing speeds, but a table or other stable horizontal surface needs to be available. As with smartphones, the current generation of viewscreens are susceptible to glare and sometimes difficult to use in bright sunlight. The development of specialized voice-recognition vocabularies could allow the use of speech-to-text software for filling in forms and reports.

Web browsers running on tablets are entirely capable of producing readable results from online searches and database queries. Customized apps could provide an even higher level of user experience, including cached data sets for use when network connectivity is lost.

Highly portable wearable units permit both hands to be free, but have limitations due to their minimalist user interface. Nonetheless, they can be very useful for still photography, short-duration video segments, and audio recording of verbal notes, interviews, or other sounds.

While large amounts of text cannot be read on these small screens, text-to-voice technology is making it possible to have the system read material aloud via earbuds or bone conduction transducers.

Software like Skype, Google Hangouts, or Apple’s Facetime can enable real-time two-way video-teleconferencing and even desktop sharing to the device.

Route-finding and tracking may be performed with maps or satellite imagery showing real time position and heading.

## 3.3 Use case #2—Measurement and Sampling

Because measuring and taking samples can be elaborate processes and need to be technically precise, using mobile devices can expedite the work and simultaneously provide confidence that the measure or sample was properly taken. Third-party tools can greatly extend the basic capabilities of these computers.

As with the inspection support use-case, some situations will limit or prohibit some or all use of portable computers due to the potential to release sensitive information. The same concerns and possible remedies mentioned in section 4.2 apply here.

Smartphones conceivably could be used by one party to record the measuring or sampling activities of another person. Either still or video photography could document this and the results shared with the other party.

Of potential interest in this area, recent advances in 3-D surveying have led to commercial add-on products for smartphones that rapidly and automatically generate accurate digital models of interior spaces. See for example the Structure Sensor (www.occipital.com). Such technology has the potential to greatly speed up certain types of activities such as IAEA Design Information Verification (DIV) inspections.

Although larger than smartphones, tablet computers bring essentially the same capabilities to the OSI party. With the possibility of an external keyboard, data entry becomes easy if less portable. Larger screens on tablets make maps, facility diagrams, floor plans, and other geospatial information easier to read. Placing maptacks with associated information on a GIS app can be done more accurately on the larger tablet interface. Usability of geospatial information is much greater on tablets than smartphones (http://www.nngroup.com/articles/mobile-maps-locations/)

Especially in the case of sample taking or placing tags and seals, both hands must be free to manipulate the tools and objects involved. Hands-free systems have the potential to permit remote viewers to aid in the selection of a sample location, to witness the collection of the sample, and to provide expert advice or how-to information to the on-site personnel.

## 3.4 Use case #3—Managed Access

Managed access represents the techniques and methods by which an Inspected State Party can demonstrate compliance with a treaty or agreement while still protecting sensitive information unrelated to the inspection mandate. While the Inspected State Party may deny either full access or requests for access to specific areas or items, it may offer alternatives such as constrained viewing, shrouding, provision of alternative information, random access to a subset of locations, and sampling instead of full access. Portable digital information systems can assist with these standard activities and add new capabilities to the inspection toolbox.

With their GPS systems, smartphones are able to track inspection party location and, with a suitably configured app, could alert one or both parties when managed access areas are approached. Escorts could be informed of the exact location and nature of sensitive information, materials, processes, and areas.

When an area cannot be entered by inspectors, it may be possible for the Inspected State Party to substitute a live video stream from a mobile device whose location and authenticity can be assured. Video of this nature could substitute for constrained viewing of an area, since the point of view is controlled entirely by the Inspected State Party, but must be validated.

Sampling is another managed access technique that can replace direct physical inspection. Paired devices with a live two-way video feed could allow inspectors to witness the taking of a sample without entering an area. This would greatly increase confidence in the process and allow stronger compliance conclusions to be made.

The iObserver platform under development at Sandia performs a telepresence inspection by providing a secure, authenticated audio, video, and data sharing channel between a facility to be visited and virtual site visitors in a remote location. It is designed as a confidence-building measure (Forden 2014). iObserver is meant to introduce countries that have little experience with international on-site inspections to OSI modalities, managed access techniques, and treaty verification. The iObserver system is designed to operate primarily on an iPad Air or Mini.

If telepresence inspections operated by the Inspected State Party can be used in place of some proportion of physical inspections by foreign nationals, mobile devices have the potential to actually reduce the likelihood of the release of sensitive information while still revealing treaty-relevant information. Future research to estimate numerically the trade-offs between telepresence and physical inspections would be worthwhile.

In situations where the Inspected State Party is providing a video stream to inspectors, augmented reality systems could dynamically shroud or virtually redact features from a video in real time. Both parties would have to validate the software and hardware systems in order to have confidence in the process. Prototype apps have successfully tracked and dynamically shrouded small 3D objects as the viewer and the object are moved about. See section 5.3.1 for additional details.

As for alternative information, it could be readily supplied wirelessly from the inspection operations center and delivered in a timelier manner to teams in the field instead of dealing with cumbersome paper records.

## 3.5 Use case #4—Training

Mobile computers are changing the face of education and training of inspectors, escorts, and policy makers in ways that could be scarcely imagined ten years ago (http://pewinternet.org/Reports/2013/Teachers-and-technology.aspx). Digital technologies are enabling trainees and students to have access to more and varied information, interact with a wider audience, encourage greater collaboration, and enhance opportunities for interaction with a

larger population of instructors and students. For example, Sandia's International Training Course (ITC) on the physical protection of nuclear materials typically instructs about 40 students in a face-to-face setting with a core group of about six instructors (Overholt 2014). Use of mobile devices could extend the learning experience to include off-site instructors, interaction with past student participants, and access to live video of remote training facilities such as Sandia National Laboratories' Integrated Security Facility. Similar advantages can easily be imagined for training inspectors, hosts, escorts, and policy makers.

Smartphones can permit distance learning via video-teleconferencing, podcast, or streaming audio-video. They can assist with learning complex procedures via augmented reality in which a virtual object is manipulated in a camera view of a real learning environment. This permits a safe and secure learning experience without the hazards associated with the actual process. "Serious gaming" can introduce complex situations in real time. Smartphones can readily access online learning or testing material, but consuming large amounts of text can be a strain on the operator. Due to the device's portability, training activities can fit in with the user's schedule or take place during normally unusable time, for example, while traveling.

Training systems that make use of mobile technology are becoming common and tablet computers as e-readers are replacing textbooks in many cases. Sandia is using iPads as an integral part of their ITC. Not only does the iPad obviate the need for large binders full of hardcopy class materials, but it permits access to a highly detailed virtual training facility. As with smartphones, tablets can permit distance learning via video-teleconferencing, can assist with learning complex procedures via augmented reality, can host educational games, and can readily access online learning or testing material.

While wearable systems are currently less effective in delivering traditional learning content in a sit-down classroom setting, they offer a number of useful capabilities in a teaching laboratory or during on-the-job training. Instructors can get a "student-eye view" as work is performed. Real-time feedback can be given and question-answer dialogs can take place. Augmented reality can in effect "show" a trainee how a mechanical process should be carried out step by step.

## 3.6 Other OSI-related Uses for Mobile Computing Technology

Besides the OSI activity itself, mobile technology can add value to other aspects of the arms control/treaty compliance process. In particular, mobile computing can assist with decision support and inspection planning as well as OSI training. However, in all these applications it is important to emphasize the need for data assurance. Making decisions or organizing training around flawed or incomplete data could produce serious consequences.

Computer-assisted training for various OSI scenarios has been available since the 1990s (Dobranich et al. 1997; Callahan 2011). Initially, these relied on the power of a desktop computer to display virtual reality imagery and to connect training exercise participants. More recently, OSI training systems make use of VR helmets and laptop computers to provide a more realistic interactive environment. One can expect steady improvements in these kinds of systems as mobile computing platforms continue to gain in power and shrink in size.

Inspection preparation tools deployed on smartphones and tablet computers could help Inspected State Parties make accurate declarations by comparing inventory at the site to host accounting records. Meanwhile, facility databases could be available to field workers to better enable them to prepare inspection materials, documents, and plans. Security and safety personnel could more effectively perform pre-inspection walk-throughs and post-inspection assessments. Past inspection data would be easily accessed, easily sorted through, and presented intuitively based on the context of the mobile user.

Mobile computing platforms offer the potential for assisting with decision support. For either party, timely access to information about the state of an inspection, the inspected facility, and its declaration could allow off-site decision makers to make sensible and informed choices about how to best conduct the inspection. Questions about inspection routes, what to photograph or sample, who to interview, and how to most efficiently use limited time on site could better be addressed by team members at the operations center when they have a more complete and realistic understanding of the situation based on inputs from mobile computers with their numerous sensors and communications channels.

Another possible use of mobile technology is its application for crowdsourcing verification. Rose Gottemoeller of the U.S. State Department has promulgated the use of “public verification measures” by private citizens with their “ubiquitous sensing devices” (Gottemoeller 2013a; Gottemoeller 2013b). The State Department has taken this a step further by offering cash prizes for crowdsourced challenges (State Dept 2013; Center for Strategic and International Studies 2013). Instead of Inspected State Party or Inspection Team personnel, members of the general public are the ones making use of their mobile devices to help solve arms control and verification questions.

# 4. IMPEDIMENTS, RISKS, AND MITIGATIONS

As a result of the range of capabilities potentially available in a small integrated package, there are numerous hurdles to be overcome before mobile devices are allowed into the on-site inspector's toolkit. Considering that treaty regimes usually specify in detail the equipment that inspectors will be permitted to use, device approval will be a critical step. Of course, site owners may easily authorize their escort's use of mobile, but the inspection team will not usually have this freedom. However, the boundary between cell phones and other common devices is blurring. For example, hearing aids now often feature Bluetooth wireless connectivity. "Smartwatches," Wi-Fi enabled health monitors, and other small, wearable devices are available.

Intrusiveness and the associated potential to put non-treaty relevant sensitive information at risk are probably the largest hurdles to overcome. Allowing these small but powerful computers into a facility will require forethought and planning, even if they are under host control.

In many use cases a solution to the intrusiveness of a mobile device is to use devices with certain features disabled, for example, camera and/or Wi-Fi. While this solves the intrusiveness problem, it removes useful capabilities. Research into developing a photo app that disables video recording when within a defined area could avoid the necessity of fully disabling a smartphone's camera. The app must be shown to work flawlessly even if the GPS signal is lost or under other circumstances. Perhaps a perimeter of wireless pylons could monitor signals and automatically moderate which features of a device are enabled or disabled. For example, the ability to automatically switch to "Airplane Mode" in places where network protocols should be disabled would be valuable. Much additional research is needed before such strategies can be implemented within a genuine inspection regime.

Even without purposely disabling features, some capabilities are limited by the environment. Currently, GPS is greatly hindered inside structures, particularly multi-story metal structures. (Even cell phone reception can be limited or blocked in interior spaces.) Advances are being made to develop chips that use one's last known GPS position plus direction, gait, and time, laser rangefinders, or trilaterate from Wi-Fi receivers to estimate location within a structure ("APL Backpack-Sized Mini-mapper Captures Intel in Tight Spots" 2013).

Lost signals and dead zones are a common problem with normal cell phone use. Many facilities of interest to on-site inspectors are in remote locations and may have intermittent communication service at best. Apps need to be designed to fail gracefully, collect information when offline, resume uploading when back online, and operate with some onboard capability even when out of network. However, real-time off-site communication for the inspection team may not be desirable from a host perspective.

Controlling data flow to mobile computers is another aspect in need of consideration. In some use cases the host may not permit data to stream off-site without review, if at all. Data volumes could be very high, especially if streaming video or real-time sensor data is involved. Apps will need to be built to throttle their data appetites, whether sending or receiving, so that critical real-time functions are not slowed or halted and so that adequate storage space is maintained. Battery

life becomes an important consideration when continuously operating energy-consuming features like screen illumination, GPS, background processes, and camera.

Similarly, synchronization with off-site databases has to be performed such that needed information is available in a timely manner while avoiding overloading available bandwidth. Downloads to offsite servers could be postponed until after the inspection, uploads could be performed ahead of time, and only transactional records posted in real time.

Information security will always be a concern with any OSI technology. Information authentication, validation, verification, and other aspects of security cannot be overlooked in these situations. Sensitive information must only be accessible to authorized recipients, data streams must be protected from accidental or purposeful alterations. Contingencies should be made in the event that a mobile device is lost, stolen or confiscated. The possibility of communication disruption could result in a failed inspection.

A general list of risks events, consequences, and mitigations is given below (Pinsonneault 2014). These are technical consequences only, which do not take into account political consequences that could occur should a particular compromise take place. Such political consequences are beyond the scope of this paper.

**Table 2 Risks, Consequences, and Mitigations**

| | Event or Condition | Consequence | Mitigation |
|---|---|---|---|
| **1.** | A mobile device is lost or stolen and the finder keeps it for personal use or sale. | Unauthorized access to inspection-related information. | Remote device locating and data wiping software installed. Remote data storage protections for apps that store data on a shared web platform. |
| **2.** | A mobile device is present in a sensitive area or during a sensitive conversation, meeting, presentation, walk-through, or other inspection activity. | Potential loss of information via mobile device's cellular service, camera, or microphone and recording software. | User awareness training; signage; confiscation of device by facility owner. |
| **3.** | Mobile device owner "jailbreaks" or otherwise customizes their device. | Violation of policy. Potential system instability. Potential for unauthorized access by unprotected SSH server installed on device. Potential for installation of malicious apps. | Standardized configuration reset upon each inspection. |

| | | | |
|---|---|---|---|
| **4.** | A confiscated, lost or stolen mobile device is jailbroken. | Additional access is given to the mobile device's file system. Encrypted areas of the file system and app-specific encrypted enclaves may be subjected to brute-force passcode attacks. | Remote locating and data wiping software installed. Remote data storage protections for apps that store data on a shared web platform. |
| **5.** | Mobile device owner syncs SUI to cloud-based storage. | Weak security (weak user password or poor security on the part of the cloud provider) or a legal discovery demand not related to the owning agency could result in unauthorized access to SUI. | User awareness training; standardized configuration reset upon each inspection. |
| **6.** | Remote adversary penetrates a mobile device and/or the agency infrastructure that supports the mobile device deployment. | Adversary potentially has access to or the ability to alter data stored on mobile devices from across the agency deployment, possibly including user location data, phone/message logs, and stored contacts. | User awareness training; standardized configuration reset upon each inspection. |
| **7.** | Apps containing malicious/questionable code are installed from an Apps Store by mobile device users. | Information such as user location, phone logs, SMS messages, contacts, and SUI stored on the phone is exfiltrated to locations not within the owner'scontrol. Avenues for additional attacks may be opened due to app weaknesses. | User awareness training; standardized configuration reset upon each inspection. |
| **8.** | Mobile device management (MDM) software installed on the owning agency's network contains vulnerabilities. | An adversary can exploit these vulnerabilities, possibly remotely via mobile devices, to gain access to the agency's computing environments. | Air gap between MDM systems and general agency networks. |

| | | | |
|---|---|---|---|
| **9.** | Mobile device users connect their devices to non-agency owned/controlled equipment to facilitate battery charging (this equipment may not necessarily be non-agency owned computers). | This situation possible because users are typically unaware that battery charging requires a full data connection via USB. This provides adversaries an opportunity for mobile device exploitation. | User awareness training; standardized configuration reset upon each inspection. |
| **10.** | Mobile device use is unsafe. | Mobile device use is unsafe due to combustible atmosphere, likelihood of user distraction, possibility of contamination, or other health and safety issue. | User awareness training; formal hazard assessment. |

Because traditional calculations define risk as the product of probability and consequences, it is necessary to look at both factors in the risk equation when considering potential threats. Whatever the situation, sensitive information needs to be confidential, encrypted, authenticated, validated, timely, and reliable whether being used, transmitted, stored, or jointly shared.

## 4.1 Inspected State Party Perspective

The hosts or escorts involved in OSI activities may have more enabled features and sensitive data on their devices simply because they are trusted and the devices can be completely controlled. This could place these devices at higher risk because the consequences of loss or compromise of this larger body of potentially sensitive information are higher. Transmission, storage and use of sensitive OSI information need to include all aspects of information surety (confidentiality, encryption, authentication, validation, performance, and reliability).

At the same time, mobile devices owned by the host may be restricted to on-site use, which would lower their risk because the probability of loss or compromise is lower. Items 1 and 4 in Table 2 deal with lost or stolen devices and those risks could be reduced by restricting off-site use of devices involved with OSI escort duties. Perhaps a rigorous check-in/check-out process could be implemented as an administrative control.

However, this might not be practical in all situations. If off-site loss or theft is possible, devices should have their screen lock enabled and have a remote location/data wipe feature installed so that the equipment may be located if lost or information can be deleted if it is stolen.

## 4.2 Inspection Team Perspective

Inspectors operate in three states with regard to mobile computing equipment: (1) on-site during the OSI activity, (2) off-site but performing OSI-related tasks, and (3) off-site at other times not during conduct of inspection activities (i.e., while in transit to/from the inspection site).

In the first case, allowed devices may be provided by the host[1] and/or be limited in functionality. While this may lower the overall risk because less information is stored on the devices, what information is there could be at risk of interception by a determined adversary. Data on host-provided equipment would almost certainly be expected to become known to the Inspected State Party when the equipment is returned at the end of the OSI event.

In the second case, inspectors may be using agency-supplied equipment to conduct OSI-related work offsite. This exposes the users to all manner of risks, from theft or loss to wireless attacks by third party adversaries (not necessarily the Inspected State Party).

In the third case, inspectors are usually protected under the 1961 Vienna Convention on Diplomatic Relations in addition to any protections provided by negotiated inspection annexes or protocols. While that minimizes the possibility of seizure by the Inspected State Party or any authority encountered while in transit to the inspection location, there is still the chance of loss or theft of a device in a public place.

## 4.3 Deployment Options

There are a wide number of options for use of mobile devices that correspond to various strategies already developed for applying single-use technologies in transparency, verification, and compliance situations.

- Facility-owned and supplied equipment for hosts/escorts only
- Facility-owned and supplied equipment for inspectors only
- Facility-owned and supplied equipment for both parties
- Inspection Team-supplied mobile devices for their own use
- Inspection Team-supplied mobile devices for facility operator use during OSI

Inspected State Party-owned equipment, while exposing some risks, can be configured to mitigate various threats (Table 2). Because the equipment is under the continuous control of Inspected State Party personnel, there is minimal danger of misuse. For example, a strategy of deploying facility-owned device to staff working within controlled areas while disabling camera and audio-video recording and only permitting Wi-Fi connectivity in designated hotspots leaves the mobile device limited to on-board applications and data, voice telecommunications, and data transfer by means of the cellular network.

Whichever party provides the equipment, a verification process needs to be in place to ensure that no malicious hardware or software has been introduced, either intentionally or accidentally. One option is for the party supplying the equipment to provide more than the required number of mobile units. The other party may then randomly examine and test a sample of the devices.

Whatever strategy is employed for approval, it may be the case that equipment, once introduced to an area, must remain in that area. Physically locking mobile devices in an appropriately tagged

[1] Use of equipment provided by the host would be a new precedent with significant implications for trustability of data collection/processing capabilities. If such a step were to be taken, the inspecting party would need some process for assuring that this equipment operates as expected.

and sealed secure enclosure would help ensure that the equipment was not tampered with between inspections.

There have been inspection regimes wherein the inspectorate controlled the equipment used on OSI missions, particularly regimes enforced as a result of a conflict. It could be possible to use smartphones and tablet computers in such situations, although consideration should be given to a possible misperception that the devices are "espionage" equipment.

# 5. FIELD STUDIES

## 5.1 Proof-of-Concept Field Exercises

As part of this research, Sandia National Laboratories has undertaken to explore the utility of mobile computing devices in an illustrative OSI environment with a prototype item tracking system in two surrogate bunkers (labeled 8013 and 8015). The site was selected because it has areas and items that are appropriate surrogate targets for generic safeguards or arms control inspection exercises.

### *5.1.1 Notional Weapon Storage Scenario*

Warheads and containers in a bunker are declared items under a generic treaty or agreement. An OSI is to be carried out to verify the correctness and completeness of their declaration. An inspection team member along with an escort team member will conduct the inspection beginning at the point of entry (POE) at the access road. Managed access will be used by the host to ensure that equipment and areas unrelated to the agreement are not compromised.

### *5.1.2 Experimental*

Eight items have QR coded tags applied prior to the exercise. Observers will accompany the members of the inspection group in order to make notes, measure elapsed time, and monitor the activities. After-action analyses will assess gains or losses in effectiveness, efficiency, safety, and security.

### *5.1.3 Activities*

In all cases observers will record activities undertaken and the time required for completion as well as any comments on unscripted situations that occur. Scenarios 1-7 below summarize the questions to be answered and the corresponding activities.

1. *What is the baseline effort to carry out the inspection?* Conduct the inspection from the POE to the inspectable item (warhead or container) and return as scripted without the use of any mobile technology.
2. *What is the value of still photography?* One member of the escort team will use the mobile device to take photographs during the inspection. The combined work product will be evaluated after the exercise is completed.
3. Repeat activity 2 with the inspection team using the mobile device.
4. *What is the impact of mobile devices when used by the escort team for video recording the entire inspection?* The escort team member will take a complete video of the inspection (without real-time transmission). The video will be evaluated after the exercise is completed.
5. *What is the value of inspection tracking with mobile devices?* The escort activates an inspection tracking app using GPS on their mobile device. At the end of the inspection, the location traces and timestamps will be compared with manual notes taken by the observers. Special attention will be given to assessing the effect of loss of GPS signal within structures.

6. *How can QR codes be used to expedite OSI?* QR codes will be placed in the inspection area encoded with (a) plain text and (b) a URL to a relevant webpage. Escorts and inspectors will interrogate the QR codes with a standard QR reader app. The time to obtain information encoded in the QR codes will be compared with the time required without their use (from the baseline scenario).
7. *Can mobile devices assist with managed access situations?* In response to an inspector's request to enter an area, the escort provides alternative without the inspector entering or directly viewing the area in question. After-action discussion will consider the effectiveness and efficiency of the process.

**Table 3 Summary of Scenarios and Activities (S1-S7)**

| Mobile Feature | *S1 (Baseline)* | *S2/S3* | *S4* | *S5* | *S6* | *S7* |
|---|---|---|---|---|---|---|
| **Still photography** | | X | | | | X |
| **Video-recording** | | | X | | | X |
| **GPS** | | | | X | | |
| **QR codes** | | | | | X | |
| **Database access** | | | | | X | |

## 5.2 Results

After conducting the mock inspection both with and without mobile devices, a hot wash was convened to capture lessons learned.

### *5.2.1 Video recording*

In our research, we found full length video of an OSI event to be impractically large for smartphones and wearable devices. Dedicated video cameras like the GoPro are better suited to that level of video documentation. Shorter video clips that record specific activities of limited duration are much more practical for devices with less than 10 GB of onboard memory.

During the exercise, a Sandia videographer (Figure 2) recorded the activities and interactions with professional-grade equipment. Additional video from the field exercise is available separately.


**Figure 2 The inspection facility used for the exercise and our videographer**

**Figure 3 Interior view of Bunker 8013 showing north (left) and south sections**

### *5.2.2 Digital photography and audio notes*

Stand-alone photography can be a valuable capability for documenting OSI activities. Still photography does not suffer from the file size limitations of video recording mentioned above. Large numbers of still photographs can be taken and easily stored with the current generation of smartphones, tablets and wearable devices.

Photographs of entire items (approximately 3'x 5') lacked sufficient sharpness to provide readable text of the 0.2" (3 mm) high item labels. Consideration should be given for a large enough font size relative to the dimensions of the items of interest when labels may need to be legible in photographs.

Audio recording and speech recognition in laboratory tests worked well in quiet environments. However, Google Glass fails to transcribe without a data connection. Inside Bunker 8013 where there is limited cell service and no Wi-Fi connection, the Endnote app would not record and transcribe to text. Pure sound recording apps are able to work in a stand-alone mode, but required separate manual transcription.

### *5.2.3 Mobile video-conferencing*[2]

Once again, the lack of cellular phone service or Wi-Fi prevented the functioning of Google Hangouts during the inspection of the bunker. Additionally, the use of a commercial service introduces possible security concerns about intercepted transmissions of either wireless or Internet channels.

Skype or Apple FaceTime as alternatives to video Hangouts also require a cellular or Wi-Fi connection and would suffer from the same limitation.

[2] The use of such a capability would need to be negotiated and consideration given to whether it violates any limits on the number of inspectors allowed to be present for an inspection.

### *5.2.4 Inspection tracking*

GPS is reliable and accurate in outdoor locations, but 8013's poor reception of satellite signals meant that interior locating was limited. A simple GPS app had error circles large enough that the very similar bunkers 8013 and 8015 (separated by about 100 yards) could not be definitively discriminated.

However, a COTS GPS tracking program (MapMyWalk) was able to accurately follow the inspection team from the site perimeter to the inspection bunker. Figure 4 shows the inspection route from the green marker at the site perimeter until the inspection was completed at the red marker. It demonstrates that this app could unambiguously identify the inspected structure. Additional information provided by the app were elevation, pace, and timestamp at any point along the route. As with other mobile apps, the thick walls of the bunker blocked external signals and there is no GPS trace of activities in the interior of the facility. Instead, the app simply "connected the dots" resulting in a long period with no change denoted by the long section of horizontal red and blue lines in the time graph at the bottom. This manner of dealing with a loss of GPS signal would not be desired in an inspection tracking app, since one would need to accurately know when and where signals were dropped and regained.

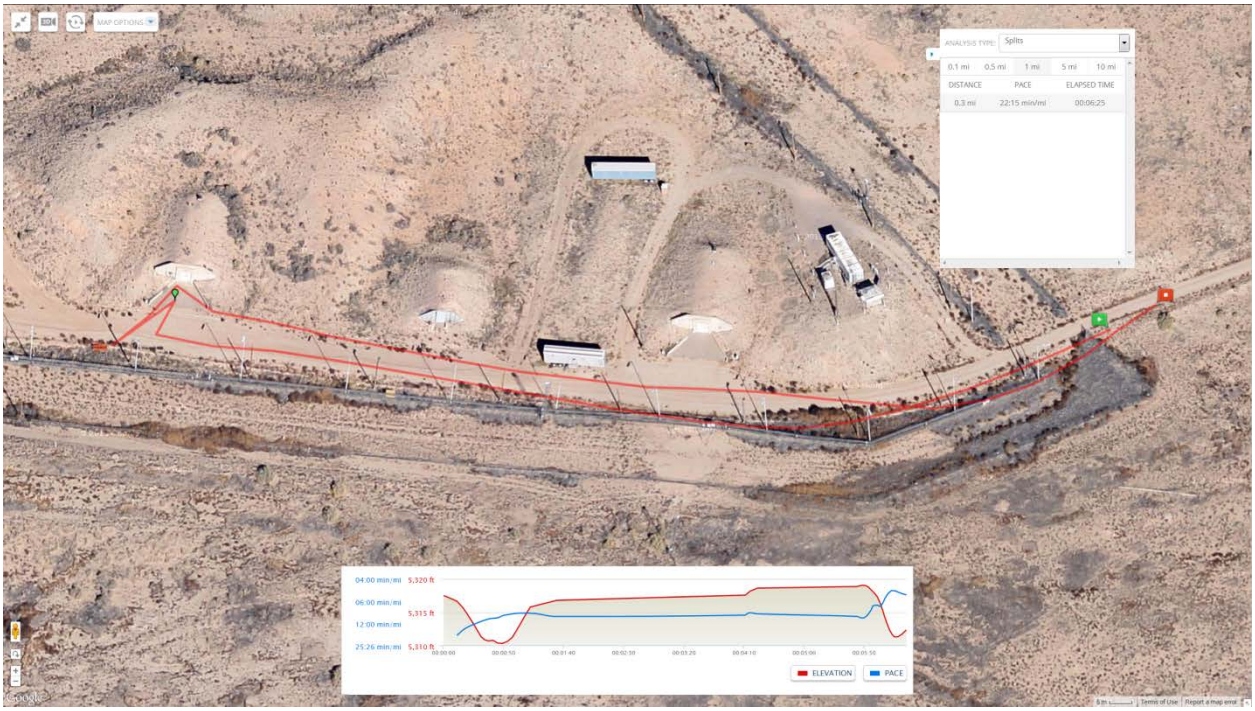


**Figure 4 Sample output from a COTS GPS tracking app**

### *5.2.5 QR codes*

With an appropriate reader, QR codes can be easily and reliably read. Straight text can be read directly, but URLs that pointed to external resources (websites, Google maps) failed when a data connection is absent. Figure 5 shows a screen capture of a COTS QR code reader app that has an associated inventory database. The product ID is the URL that links to detailed item information. QR codes were 3.25" (8.5 cm) square.

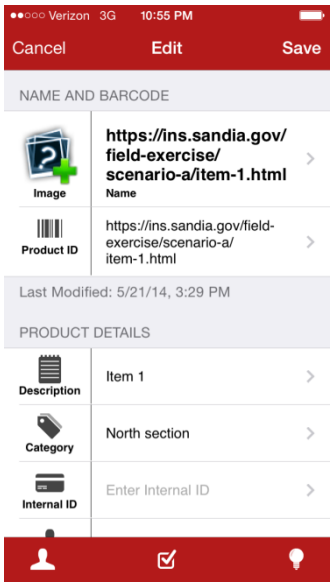


**Figure 5 Screen capture of QR code-based inventory app**

### *5.2.6 Managed access*

The limited data connection in 8013 prevented the use of direct video-teleconferencing via Google Hangouts or other such system. The alternative we chose was for the host to use stand-alone digital photography to capture relevant images of undeclared items and then share them immediately with the inspector. This was deemed transparent and helpful, but not sufficient for actual verification purposes. Figure 6 is a view of two items of interest that were not declared for one part of the exercise, while Figure 7 shows the north half of the facility. Even in the brighter parts of the bunker, slow exposure time, hand vibration, and low resolution made it difficult to capture recognizable item numbers while showing most of the object. The use of much larger fonts is recommended on labels.


**Figure 6 Mock undeclared items**

**Figure 7 General view of inspection area**

### *5.2.7 Time to complete activities*

Based on our mock OSI activities (Table 4), we found smartphone apps were actually slower than manual processes. Selecting menus and data entry in a mobile app were slower than

making handwritten notes. This has important implications when rapid completion of an inspection is a high priority, for example, when radiation levels are a concern. However, post-inspection data processing to transcribe written notes would be slower and more prone to error when compared against an electronic transmission of a completed digital inventory.

**Table 4 Elapsed Time for Activities**

| Activity | Baseline | With smartphone |
|---|---|---|
| **Confirm inspection location** | A few moments | A few moments |
| **Confirm declared inventory of items** | 1.75 min | 3 min |
| **Take sample measurements** | 38 sec | 1:21 min |
| **Managed access** | 4:45 min | 2:03 min |

### *5.2.8 Google Glass*

Wearable technologies such as Google Glass offer the potential for more complete documentation of the inspection process with hands-free operation. After the mock inspection using an iPhone as the mobile device, Google Glass images were taken in the facility for comparison. Most notably, the hands-free aspect allowed one to capture activities that would be awkward at best using a hand-held camera. In Figure 8 an inspector takes a GPS reading and compass bearing. Figure 9 illustrates the use of an HM-5 meter as seen through Glass.

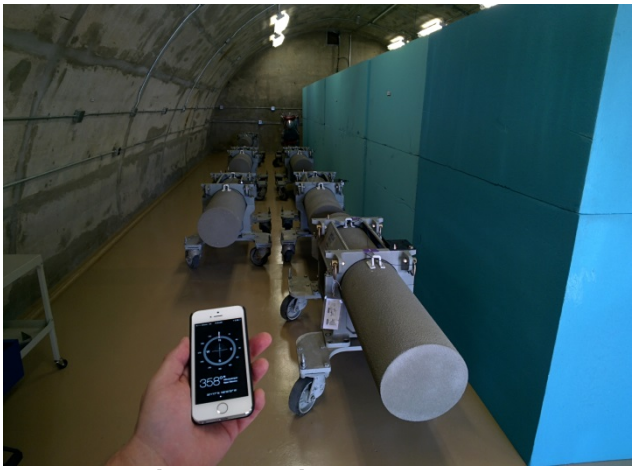

**Figure 8 Using a GPS app**

**Figure 9 Taking a radiation measurement**

### *5.2.9 Overall*

Mobile technologies are not a universal panacea for all OSI problems. One must take into account the inspection environment, user background, behavior, role, cultural aspects of the countries involved, as well as specific treaty agreement and facility constraint issues. Many environments (including weapon storage facilities) have significant constraints on the operations of electronic devices for safety reasons. The use of such technologies, if possible, would require significant safety reviews and assessments.

Our work with COTS devices operating COTS software and apps suffice to demonstrate that mobile technologies are capable of carrying out a number of OSI-related tasks, but they may not be able to out-perform traditional manual methods. A more thorough test and analysis with appropriate training would be needed to determine if one mode was advantageous. Our exercise

was illustrative rather than definitive. Security concerns with multifunction devices make stand-alone tools, such as dedicated GPS devices or standard digital cameras, easier and safer to use and manage in sensitive environments.

## 5.3 Additional Proof-of-Concept Exercises

### *5.3.1 Augmented Reality Applications*

The earliest AR apps used a smartphone's camera, GPS and compass to place location-specific information on-screen. For example, a simple AR app has been developed that identifies buildings at Sandia as shown in Figure 10 below.

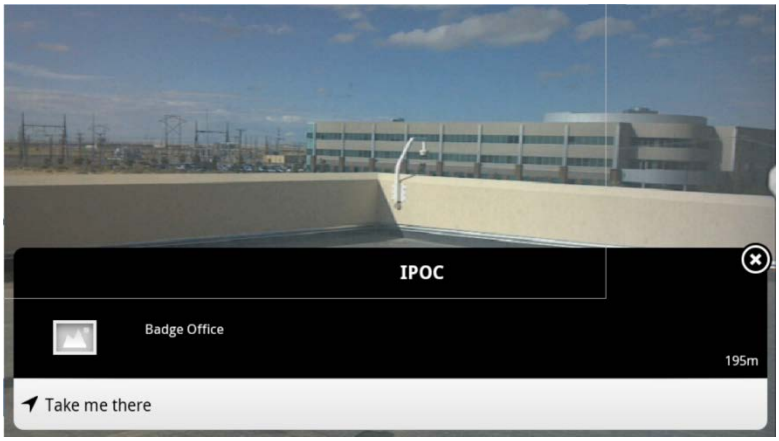


**Figure 10 Screen capture of an AR app identifying a building**

A more advanced application of AR is to render a 3-dimensional shape within the viewscreen when the app recognizes a particular feature set. Such a feature set becomes the frame of reference for the coordinate system that permits accurate placement of the virtual 3D shape within the view.

In a managed access situation, this capability allows for novel uses. One that we have investigated is digital redaction or virtual shrouding. The 3D shape that is rendered in the view screen is an opaque object larger than the item of concern. In Figure 11 a prototype app is shown that displays a shrouded cuboid in the camera viewscreen while the actual item is visible beyond in the operator's left hand.

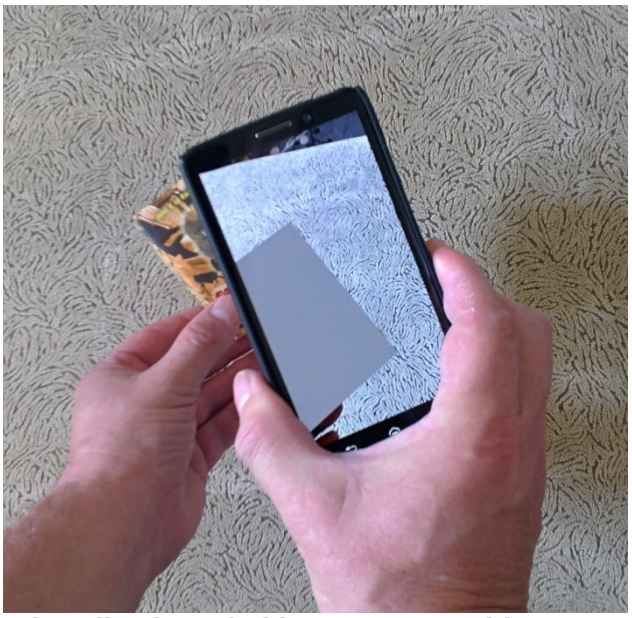

**Figure 11 A virtually shrouded item as seen with a smartphone app**

A large number of items of interest that might conceivably require virtual shrouding are cylindrical (Table 5). With that in mind, we set out to develop a generic cylindrical virtual shroud. By using an opaque cylinder with an aspect ratio of 2 to 1, the app can shroud 6 of the 7 test items. Only TRIS (TRusted Information System) is longer and narrower than a 2:1 virtual shroud. Viewing TRIS with the prototype cylindrical virtual shroud app would leave portions of the device exposed at either end as the virtual shroud is not long enough relative to the object's width to conceal it entirely.

Most cylindrical objects in our testbed are relatively featureless, often painted a uniform color with very few features that could be used as the basis for anchoring the coordinate system of an AR app. To overcome this paucity of alignment features, we created a cylinder target that would be placed approximately in the middle of an object of concern in a belt-like fashion. When viewed with the corresponding augmented reality app, the object appears to be surrounded by a larger, opaque grey cylinder. None of the actual object of concern is visible in the camera viewscreen.

**Table 5 Dimensions (cm) of Selected Items of Concern**

| Object | Diameter | Circumference | Height | Aspect ratio |
|---|---|---|---|---|
| **Weapon container** | 82 | 258 | 150 | 1.83 |
| **Gamma detector** | 10 | 31 | 42 | 4.20 |
| **TRIS** | 17 | 53 | 30 | 1.76 |
| **AT-400** | 51 | 160 | 74 | 1.45 |
| **AT-400R** | 48 | 151 | 52 | 1.08 |
| **OSRP** | 59 | 185 | 90 | 1.53 |
| **Ceramic Seal** | 24 | 75 | 23 | 0.96 |

We continue to refine this application to overcome issues with target resolution and image latency—the item of concern briefly appears before the smartphone's camera fully recognizes the salient feature set and applies the virtual shroud.

### *5.3.2 Integrated Security Facility*

Sandia's Integrated Security Facility (ISF) hosts the Nuclear Security Center of Excellence (NSCOE), a physical security and operational safety testbed and training facility. The ISF has a Perimeter Intrusion Detection and Assessment System (PIDAS), a central command post, video monitoring, a prototype RFID tracking system, several inspectable buildings (four with Wi-Fi), and a number of areas of interest that are appropriate surrogate targets for generic safeguards or arms control inspections.

As part of this study, we conducted a 45 minute walk-through with Google Glass and an iPhone. Several dozen images and videos were taken to understand the quantity and quality of the information that could be captured. Because of the unobtrusive nature of the devices, it was possible to take photos and videos with a minimum of interruption to the flow of the walk-through. As a result, digital imagery was captured at a rate of 0.75 images or videos per minute. Samples from this activity are shown in Figures 12-15.

The key limitation during this activity was the loss of cellular signals within the interior portions of the site. The addition of cellular repeaters or Wi-Fi hotspots could mitigate this, but that would be an added cost burden on a facility unless they had pre-existing infrastructure.

In the discussion during and after the walk-through, it was remarked that mobile technology would work well as a tool for distance learning in conjunction with the NSCOE training mission. Similarly, smartphones and wearable technology would be useful for site assessment activities at certain types of facilities, especially those that already permit the use of digital cameras. It was suggested that perhaps a dedicated, secure cloud could be developed where OSI information and imagery from mobile devices could be uploaded without the need for using existing commercial cloud services.

**Figure 12 Glove boxes, overhead piping, and gantry crane**

**Figure 13 Hot cells with manipulator**

**Figure 14 Material storage area**

**Figure 15 Communications and security features visible during walk-through**

# 6. ARE MOBILE TECHNOLOGIES FEASIBLE FOR OSI?

The feasibility of mobile device use during OSI hinges on the risk-benefit calculation of the parties involved. The effectiveness of possible mitigations must be balanced against advantages to the inspection process. These benefits may include reduced interruptions to operations, increased safety, enhanced thoroughness, more effective hosting/escorting, more rapid determination of results, and more accurate recording of activities.

By and large, any one mobile feature, for example, GPS, is available as a stand-alone, single purpose device. However, the integration of so many features and communications channels within a convenient, customizable, portable package makes smartphones and tablet computers both attractive as an inspection tool and forbidding as a security risk.

**Table 6 Summary of Mobile Functionality and Possible Limitations**

| Capability | Possible Limitations |
|---|---|
| **Cellular communication** | Limited battery life, “Dead zones” in remote areas |
| **Wi-Fi** | Disallowed in sensitive areas |
| **Bluetooth** | Disallowed in sensitive areas |
| **NFC/RFID reader** | Tags may easily be counterfeited without additional tamper-indicating features |
| **Still camera** | Disallowed in sensitive areas |
| **Video camera** | Disallowed in sensitive areas |
| **Audio recording** | Disallowed in sensitive areas |
| **Barcode/QR code scanner** | Barcodes and QR codes may easily be counterfeited without additional tamper-indicating technology |
| **GPS** | Unreliable within large structures |
| **Compass** | Unreliable near large amounts of ferrous metals |

## 6.1 Feasibility for CTBT

For OSI activities within the CTBT, the inspection area can be up to 1,000 sq km and inspection activities can last up to 130 days, creating an enormous logistical challenge. A recent training exercise (DTIRP, 2013) required 120 tons of equipment. Activities the inspection team may carry out under the treaty include: position finding, overflights, visual observation, video and still photography, multi-spectral imaging (including infrared measurements), gamma radiation monitoring, environmental sampling and analysis, passive seismological monitoring for aftershocks, resonance seismometry and active seismic surveys, magnetic and gravitational field mapping, ground penetrating radar, electrical conductivity measurements, and drilling.

Mobile computing technology not only can assist with inspection-specific activities, but also help with equipment tracking, personnel management, and ensuring the safety of participants in remote locations.

A single overflight is permitted under the CTBT for general site orientation for the inspection team. The equipment that can be used during the initial overflight including field glasses, passive location-finding equipment, video cameras and hand-held digital cameras, and gamma detectors.

During an OSI, the Inspected State Party will have certain rights to protect sensitive installations and locations, such as designating four-square kilometer maximum exclusion zones and up to a total of 50-square kilometers of restricted-access sites.

In addition, measures allowed under the CTBT to manage access include:

- Shrouding sensitive displays, stores, and equipment;
- Restricting measurements of radionuclide activity and nuclear radiation to only enable the inspectors to determine the presence or absence of relevant radiation and energies;
- Restricting sampling procedures to only allow inspectors to determine the presence or absence of radioactive or other relevant products;
- Managing access to buildings and other structures; and
- Declaring restricted-access sites.

In the event of a CTBT OSI, potential security concerns would arise. Security risk factors to consider at specific sites and facilities include the length of time an inspection team would be physically present on site and the inspection team's level of access to specific facilities and programs, the instruments and inspection equipment used, and the types of inspection activities conducted. Under the CTBT, these concerns would be somewhat mitigated by the probability that OSIs would most likely occur in remote, non-industrial locations.

The use of mobile technology by a CTBTO inspection team is, therefore, feasible outside of restricted-access areas although capabilities would be limited to local, on-board applications due to the remoteness of the facilities.

## 6.2 Feasibility for FMCT

The Fissile Material Cutoff Treaty (FMCT) offers a potential opportunity for the introduction of advanced mobile computing capabilities since the treaty is still in the drafting stage but there are challenges because of the nature of the activities to be observed. Two significant drafts of an FMCT have been submitted to the Conference on Disarmament: a U.S. draft that had no verification regime and a joint Japanese-Canadian-Dutch draft that proposes the IAEA verify the agreement. Verification measures could include OSI activities and States Parties might have to declare inspectable sites. These sites would likely include civilian and military nuclear facilities, uranium enrichment plants, and plutonium reprocessing plants. Challenge inspections could also be allowed. OSI activities would likely focus on verifying a State Party’s declarations in order to detect clandestine production or diversion of fissile materials. Exceptions might be made for legacy stocks, end-use stocks produced after the treaty's entry-into-force, and fissile material produced for peaceful purposes, such as naval propulsion fuel or spacecraft power.

Because nuclear facilities, enrichment plants, and reprocessing plants have sensitive technologies, security features, and processes, even civilian ones will have sizable restricted

areas. Military facilities will be even more closely restricted. Currently, it is highly unlikely that mobile computing devices would be permitted within these areas.

In order to support declaration verification inspections or potential challenge inspections, States Parties would do well to consider standardized mobile equipment that provides a modicum of data access but are disabled sufficiently to ensure security of inspected facilities. If the IAEA were to be the verification entity, the mobile technology should follow their joint use guidelines and best practices.

## 6.3 Feasibility for CWC Challenge Inspections

Because a CWC challenge inspection has never taken place, we consider the experience of a CWC challenge inspection exercise. During this exercise, cellphones and Wi-Fi devices were used extensively, but they were not permitted in controlled areas. Since then, specially configured Blackberries, iPhones, and iPads have been allowed within controlled areas at the exercise site. Presumably host-supplied devices would be allowed for inspection team use during a challenge inspection, if they were configured to allow only phone and e-mail communications and their cameras were disabled. A repeat of the exercise with current allowable technology would permit a then-and-now comparison.

Even if devices have audio/video recording, Bluetooth, and Wi-Fi capabilities disabled or turned off within controlled areas, these devices would be satisfactory for viewing previously downloaded data and documents, for example, the inspection mandate, site maps, declarations, standard reference materials, safety documents, and the detailed inspection plan. Even a static digital copy of a large document with an appropriate text search capability would be very helpful during an inspection.

Smartphones and tablet computers would also be useful for note taking and filling in inspection report templates. This text input would be uploaded and synchronized with the inspection team's master data store once the inspectors reach a Wi-Fi hotspot or return to the operations center. Outside of controlled areas, mobile technologies could ostensibly be put to their full use, including audio/video recording and real-time data transfers. Mechanisms for controlling the enabling and disabling of cameras and microphones might include password protecting the settings and requiring the Inspected State Party hosts to make any changes to the systems. Alternatively, a more sophisticated solution would be to remotely monitor device location by GPS and broadcast system configuration changes via cellular radio channels when approaching a sensitive area.

Wearable systems that leave the operator’s hands free have obvious advantages in chemical processing facilities where two hands are required for safely handling apparatus, using equipment, and attending to railings on stairs and ladders. Biological, industrial, and nuclear facilities could face the same safety constraints and accrue similar advantages with the use of wearable systems. However, consideration should be given to the possibility of user distraction with heads-up displays.

## 6.4 Feasibility for Strengthened Safeguards

Although the NPT does not have a verification regime and nuclear weapons states are not required to have safeguards agreements with the IAEA, all five NWS have concluded comprehensive Safeguards Agreements with an Additional Protocol. As of September 2012, approximately 180 countries have Safeguards Agreements and 125 have model Additional Protocols in force.

Facility attachments have not taken into account the rapid evolution of mobile computing devices in the past five years. It is very unlikely that States will allow highly intrusive mobile computers into sensitive facilities.

However, mobile computing could find a useful niche for host and escort support during OSI activities. Also, mobile technology can provide IAEA inspectors with information processing capabilities outside of sensitive locations and while traveling.

## 6.5 Overall Conclusions

Because facility owners may tightly control their personnel and highly customize their escort's mobile platforms, these technologies have a much broader application for the Inspected State Party. Hosts/escorts can be trained well ahead of time, equipment can be properly configured/disabled, and policies for use put in place. With well-thought-out administrative and engineering controls, it is conceivable that mobile computing devices can be brought safely and securely into even sensitive areas by facility personnel.

Inspection parties on the other hand, must operate within the often strict limitations of treaties or agreements. Under current OSI regimes, there are few opportunities for applying mobile computers to inspection team activities. Inspectors may find that these technologies are best applied in training and to make efficient use of time while en route to and from sites.

For agreements currently in force with rigorous equipment specifications, it seems doubtful that mobile devices will be allowed on inspection visits. That does not mean that in an offsite operations center or other location smartphones, tablets, and wearable systems will not be valuable adjuncts to the parties' information and communication systems. Because inspection preparation and training tasks are conducted off-site, mobile technologies have the potential to be very useful in these circumstances.

### *6.5.1 Feasibility for Future Treaties*

For future treaties and agreements whose text has not been finalized or for those with flexible equipment options, it is entirely possible to imagine safe, secure and effective use of permitted mobile devices. A number of requirements would have to be put in place for a future treaty or agreement. Some of the following would be embedded within the treaty text, while others would be practices to perform outside of the agreement.

- *Clear definition of allowable technologies.* Based on the rate of change in mobile technology, lists of specific COTS (makes and models) will rapidly become out of date. Unless there is an efficient mechanism for updating such lists of allowable makes and models, any such specification will become obsolete.
- *Allowable applications.* If necessary, apps and other code installed on the devices need to be specified. Verification and validation procedures as well as data transmission and information sharing/information protection mechanisms should be addressed.
- *Clear delineation of areas of use.* The location various devices and specific capabilities may be used needs to be defined, either by means of clearly drawn maps or in terms of some recognizable feature set. In some circumstances, time of use and/or duration of use might need to be stated as well.
- *Telecommunication infrastructure.* Any site-specific telecommunications or networking infrastructure would need to be specified unless publicly available channels are used exclusively. For structures or areas without wireless service, Wi-Fi may have to be installed as part of compliance with a future agreement or treaty.
- *Monitoring and encryption.* Mechanisms for monitoring telecommunication channels and sharing of network traffic data would have to be specified. Sharing of private keys used for encrypting information would allow both parties to have access to the data streams while protecting the data from unauthorized users.
- *Rights and responsibilities.* Individuals in possession of mobile computing devices need to be aware of their responsibilities.
- *Pre- and post-inspection procedures.* Any related processes that need to occur before or after an OSI event (equipment certification, verification, or storage under seals, etc.) should be specified.
- *Training.* Users of mobile devices during OSI need to be trained in the particulars of the specific regime in question. Such training should be documented.
- *Clear statement of disallowed uses.* Limitations and prohibited uses need to be enumerated and the consequences of unallowable use, intentional or unintentional, should be specified.
- *Resolution of anomalies.* A mechanism for resolving disputes regarding any perceived issues needs to be defined and put in place.
- *Contingencies for out-of-normal events.* Guidance should be created for use of mobile devices during an emergency, how to report and respond to damage, loss or theft of a device, or any other unusual situations that conceivably could occur.

Given that a technical description will be available for the systems allowed in any particular regime in the future, it will then be possible for operational security personnel of inspectable facilities to devise means to avoid the compromise of sensitive information. Areas that might conceivably be visited could be appropriately sanitized and network systems could be designed to always maintain adequate separation between sensitive hardware and inspection team devices. Wireless nodes to monitor digital traffic could be installed. New facilities subject to future arms control agreements could be designed to minimize the impact of mobile technologies that might be used during monitoring and verification inspections.

Over the course of this study, mobile technologies have advanced considerably. For example, since the time of submitting the original study proposal, Google Glass has become available.

Within the foreseeable future 3D spatial imaging systems and radiation detectors will likely become embedded within smartphones. Chemical and biological sensor systems could similarly be added to these devices. A mobile platform with these sorts of capabilities not only has the potential to enhance inspectors' efficiency and effectiveness, but also enable the general public to play a potential role in societal monitoring/societal verification.

# 7. RESEARCH OPPORTUNITIES AND NEXT STEPS

Throughout this report we have identified areas where research can lead to gains in our understanding of how to apply mobile technology to OSI. In Table 7 below we summarize those topics organized by the order of their appearance in this report.

**Table 7 Potential Research Topics and Follow-on Activities**

| Section | Topic | Description |
|---|---|---|
| **3.1** | Information exchange mechanisms and data authentication | Methods for verifying and authenticating jointly shared information need to designed, developed, tested, and approved. |
| **3.4** | Numerical comparison of the possibility of sensitive information loss between telepresence and physical inspections | If telepresence inspections operated by the Inspected State Party can be used in place of some portion of physical inspections by foreign nationals, mobile devices have the potential to actually reduce the likelihood of the release of sensitive information. Future research to estimate numerically the trade-offs between telepresence and physical inspections would be worthwhile. |
| **3.5** | Mobile systems for OSI training and confidence building | Questions remain about the efficiency and effectiveness of mobile devices in various training environments. Existing systems (ITC iPads, iObserver, and others) should be formally evaluated and lessons learned captured. |
| **3.6** | Crowdsourced OSI | While there have been several arms control crowdsourcing challenges online, there is still a need to explore the practical details of societal monitoring and verification. |
| **4.** | Limitations on allowable technologies | Technologies to automatically enforce restrictions on certain mobile capabilities within given areas. |
| **5.3.1** | Virtual shrouding and digital redaction | Further refinement and vulnerability assessment of an AR system to virtually shroud objects under video surveillance. |
| **6.3** | Repeat of CWC Challenge Inspection Exercise | The OSI activities of the CWC exercise could be repeated with mobile devices. Participants (especially escorts and OpSec experts) from both the exercises and the modern repeat of the inspection could provide baseline comparison of cost and benefit. |
| **6.5.1** | Formal requirements for use of mobile technologies during OSI activities mandated by future treaties or agreements. | While this report outlines in general form what would be needed to be put in place in order to implement an OSI regime that made use of some form of mobile technology or another, detailed, specific requirements need to be developed with input from stakeholders (OSI professionals, treaty negotiators, mobile technology experts, network communications professionals, and cyber security experts). |

| | | |
|---|---|---|
| **6.5.1** | Continuous assessment of new and emergent mobile technologies | With the rapid pace of technological innovation, a routine mechanism should be put in place to review new and emerging technologies. Dedicated resources can review and report on hardware and software that merit closer examination for their applicability in the arms control treaty verification domain. |

# 8. REFERENCES


*"APL Backpack-Sized Mini-mapper Captures Intel in Tight Spots."* 2013. Accessed October 23. http://www.jhuapl.edu/newscenter/stories/st130321.asp.

Bleakly, Denise, Karl Horak, and Michael McDaniel. *"Enhancing Safeguards Analysts' Geospatial Usage."* Sandia National Laboratories, SAND2012-9916.

Bray, Olin, and Sharon DeLand. 1997. *Information Model for On-Site Inspection System.* SAND97-0049.

Callahan, Paul. 2011. *"Homeland Security Initiatives"* June 27. http://www.sri.com/sites/default/files/brochures/sri-homeland-security-capabilities-preso.pdf.

Center for Strategic and International Studies. 2013. *"Arms Control and Social Networking – Crowdsourcing Intelligence."* http://csis.org/blog/arms-control-and-social-networking-crowdsourcing-intelligence.

*"Comprehensive Nuclear Test-Ban Treaty (CTBT) -- Annexes, Protocols, and Other Related Documents."* 2013. Accessed October 15. http://www.state.gov/t/avc/trty/16513.htm.

DeLand, Sharon, Tom Widney, Karl Horak, Richard Claudell, and Erick Grose. 1996. *The Interactive On-Site Inspection System: An Information Management System to Support Arms Control Inspections*. SAND93-2300.

Dobranich, Pauline, Karl Horak, David Hagan, Deborah Evanko, Jon Nelson, Christine Ryder, and Dana Hedlund. 1997. *Technical Manual for the Augmented Computer Exercise for Inspection Training (ACE-IT) Software*. SAND97–1788.

DTIRP. 2008. *"The Arms Control Inspector"*. Product No. 406P. DTIRP Outreach. http://dtirp.dtra.mil/pdfs/406p.pdf.

Finno, Roy. 2000. *"CTBT: Confidence Building Measures and On-Site Activities."*

Forden, Geoffrey, personal communication 2014.

*"Gamma Rays Caught on Camera."* 2013. Accessed April 22. http://www.rdmag.com/award-winners/2012/08/gamma-rays-caught-camera.

*"Google Glass - Home."* 2013. Accessed April 22. http://www.google.com/glass/start/.

*"GoPro Official Website: The World's Most Versatile Camera."* 2013. Accessed October 17. http://gopro.com/.

Gottemoeller, Rose. 2013a. *"Mobilizing Ingenuity To Strengthen Global Security"* March 8, SXSW Austin, TX. http://www.state.gov/t/us/205933.htm.

———. 2013b. *"Building the Future of Arms Control Through Innovative Eyes."* DipNote. http://blogs.state.gov/stories/2013/07/22/building-future-arms-control-through-innovative-eyes.

Gough, Robert, and Alan Zelicoff. 1993. *Arms Control Compliance: Information Value of Verification Measures.* SAND93-1347C.

Horak, Karl, Denise Bleakly, and Michael McDaniel. 2013. *"Advances in the Use of Open-source Information."* Accessed April 22. http://prezi.com/q3gbnizvtqf9/advances-in-the-use-of-open-source-information/.

Hung-Lin, Chi, Kang Shih-Chung, and Wang Xiangyu. 2013. *"Research Trends and Opportunities of Augmented Reality Applications in Architecture, Engineering, and Construction."* Automation in Construction Available online, ISSN 0926-5805, 10.1016/j.autcon.2012.12.017. (http://www.sciencedirect.com/science/article/pii/S0926580513000022) (January 22).

Organisation for the Prohibition of Chemical Weapons. 2005. *"Annex on Implementation and Verification of the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction."* http://www.opcw.org/index.php?eID=dam_frontend_push&docID=6357.

Overholt, Michelle Jungst, personal communication 2014.

Parrot. 2013. *"AR.Drone."* Accessed October 17. http://ardrone2.parrot.com/.

Pinsonneault, Richard, personal communication 2014.

Scheeline, Alexander, and Kathleen Kelley. 2013. *"Cell Phone Spectrometer."* Accessed April 22. http://www.asdlib.org/onlineArticles/elabware/Scheeline_Kelly_Spectrophotometer/index.html.

State Dept. 2013. *"2013 Innovation in Arms Control Challenge: What Information Technology Tools and Concepts Can Support Future Arms Control Inspections? | InnoCentive Challenge."* Accessed October 4. https://www.innocentive.com/ar/challenge/9933381.

U.S. State Department. 1987. *"Protocol Regarding Inspections Relating to the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Elimination of Their Intermediate-Range and Shorter-Range Missiles."* http://dosfan.lib.uic.edu/acda/treaties/inf5.htm.

*Wearable Computer* - Wikipedia, the Free Encyclopedia. 2013. Accessed October 4. http://en.wikipedia.org/wiki/Wearable_computer.

# 9. APPENDIX A

**Table 8 Equipment for Selected Treaties**

| | CTBT[3] | CWC[4] | Antarctic[5] | IAEA[6], NPT[7], AP[8] | BWC[9] | TTBT[10] |
|---|---|---|---|---|---|---|
| **On-Site Inspection Regime** | Challenge Inspections only | Initial, routine, challenge, and alleged-use inspections | Anytime, anywhere inspections | Ad hoc, routine, special, and unannounced inspections | None | None |
| **Equipment System for Compliance Monitoring** | System includes IMS, ancillary equipment, radiation monitors, transmission equipment, sampling devices, cameras Has an extensive list of specialized equipment Complex heavy drilling equipment | System may include sensors, ancillary equipment, transmission systems, and employ sampling devices, seals, cameras | No specialized equipment | Nuclear measurement instruments and containment and surveillance devices | None | Extensive list of specialized equipment |
| **Other** | Voluntary CBMs | Facility agreements | None | Facility attachments Additional protocols | Voluntary CBMs | CBMs |

[3] Comprehensive Nuclear-Test-Ban Treaty
[4] Chemical Weapons Convention (Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction)
[5] Antarctic Treaty and Antarctic Treaty System
[6] International Atomic Energy Organization Statute
[7] Non-Proliferation Treaty (Treaty on the Non-Proliferation of Nuclear Weapons)
[8] Additional Protocol
[9] Biological Weapons Convention (Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction)
[10] Threshold Test Ban Treaty (Treaty on the Limitation of Underground Nuclear Weapon Tests)

| | PNET[11] | INF[12] | UN Convention[13] | CFE[14] | START[15] | Open Skies | New START[16] |
|---|---|---|---|---|---|---|---|
| **On-Site Inspection Regime** | None | Close-out inspections Challenge inspections | Signatories cooperate in inspection of suspect vessels under LOS | Declared facilities Destruction process Certification process Challenge inspections | Nine types of OSI | None | Type One and Type Two inspections |
| **Equipment for Compliance Monitoring** | Extensive list of specialized equipment | Measuring, weighing, and radiation detection devices Cameras, imaging devices, and other agreed equipment | Not applicable | Cameras Binoculars Aircraft | Relatively unsophisticated OSI equipment | Cameras | Relatively unsophisticated OSI equipment, except for neutron detectors |
| **Other** | None | None | None | None | None | Aerial observation | None |

[11] Peaceful Nuclear Explosions Treaty
[12] Intermediate-Range Nuclear Forces Treaty
[13] United Nations Convention Against Traffic in Narcotic Drugs and Psychotropic Substances
[14] Treaty on Conventional Forces in Europe
[15] Strategic Arms Reduction Treaty
[16] New Strategic Arms Reduction Treaty

# 10. APPENDIX B

Relevant sections from the Protocol to the Comprehensive Nuclear Test-Ban Treaty regarding OSI ("Comprehensive Nuclear Test-Ban Treaty (CTBT) -- Annexes, Protocols, and Other Related Documents" 2013)

## Approved Inspection Equipment

36. The Conference, at its initial session, shall consider and approve a list of equipment for use during OSIs. Each State Party may submit proposals for the inclusion of equipment in the list. Specifications for the use of the equipment, as detailed in the Operational Manual for On-Site Inspections, shall take account of safety and confidentiality considerations where such equipment is likely to be used.

37. The equipment for use during OSIs shall consist of core equipment for the inspection activities and techniques specified in paragraph 69 and auxiliary equipment necessary for the effective and timely conduct of OSIs.

38. The Technical Secretariat shall ensure that all types of approved equipment are available for OSIs when required. When required for an OSI, the Technical Secretariat shall duly certify that the equipment has been calibrated, maintained and protected. To facilitate the checking of the equipment at the point of entry by the Inspected State Party, the Technical Secretariat shall provide documentation and attach seals to authenticate the certification.

39. Any permanently held equipment shall be in the custody of the Technical Secretariat. The Technical Secretariat shall be responsible for the maintenance and calibration of such equipment.

40. As appropriate, the Technical Secretariat shall make arrangements with States Parties to provide equipment mentioned in the list. Such States Parties shall be responsible for the maintenance and calibration of such equipment.

## Communications

62. The members of the inspection team shall have the right at all times during the OSI to communicate with each other and with the Technical Secretariat. For this purpose they may use their own duly approved and certified equipment with the consent of the Inspected State Party, to the extent that the Inspected State Party does not provide them with access to other telecommunications.

## Inspection Activities and Techniques

69. The following inspection activities may be conducted and techniques used, in accordance with the provisions on managed access, on collection, handling and analysis of samples, and on overflights:

(a) Position finding from the air and at the surface to confirm the boundaries of the inspection area and establish coordinates of locations therein, in support of the inspection activities;

(b) Visual observation, video and still photography and multi-spectral imaging, including infrared measurements, at and below the surface, and from the air, to search for anomalies or artifacts;

(c) Measurement of levels of radioactivity above, at and below the surface, using gamma radiation monitoring and energy resolution analysis from the air, and at or under the surface, to search for and identify radiation anomalies;

(d) Environmental sampling and analysis of solids, liquids and gases from above, at and below the surface to detect anomalies;

(e) Passive seismological monitoring for aftershocks to localize the search area and facilitate determination of the nature of an event

# 11. APPENDIX C

Relevant sections from the CWC Verification Annex regarding OSI equipment (Organisation for the Prohibition of Chemical Weapons 2005).

## Approved equipment

27. Subject to paragraph 29, there shall be no restriction by the Inspected State Party on the inspection team bringing onto the inspection site such equipment, approved in accordance with paragraph 28, which the Technical Secretariat has determined to be necessary to fulfil the inspection requirements. The Technical Secretariat shall prepare and, as appropriate, update a list of approved equipment, which may be needed for the purposes described above, and regulations governing such equipment which shall be in accordance with this Annex. In establishing the list of approved equipment and these regulations, the Technical Secretariat shall ensure that safety considerations for all the types of facilities at which such equipment is likely to be used, are taken fully into account. A list of approved equipment shall be considered and approved by the Conference pursuant to Article VIII, paragraph 21 (i).

28. The equipment shall be in the custody of the Technical Secretariat and be designated, calibrated and approved by the Technical Secretariat. The Technical Secretariat shall, to the extent possible, select that equipment which is specifically designed for the specific kind of inspection required. Designated and approved equipment shall be specifically protected against unauthorized alteration.

29. The Inspected State Party shall have the right, without prejudice to the prescribed time-frames, to inspect the equipment in the presence of inspection team members at the point of entry, i.e., to check the identity of the equipment brought in or removed from the territory of the Inspected State Party or the Host State. To facilitate such identification, the Technical Secretariat shall attach documents and devices to authenticate its designation and approval of the equipment. The inspection of the equipment shall also ascertain to the satisfaction of the Inspected State Party that the equipment meets the description of the approved equipment for the particular type of inspection. The Inspected State Party may exclude equipment not meeting that description or equipment without the above-mentioned authentication documents and devices. Procedures for the inspection of equipment shall be considered and approved by the Conference pursuant to Article VIII, paragraph 21 (i).

30. In cases where the inspection team finds it necessary to use equipment available on site not belonging to the Technical Secretariat and requests the Inspected State Party to enable the team to use such equipment, the Inspected State Party shall comply with the request to the extent it can.

# DISTRIBUTION

| | | | |
|---|---|---|---|
| 1 | MS0899 | Technical Library | 9536 (electronic copy) |


Sandia National Laboratories