HOMELAND SECURITY PRESIDENTIAL DIRECTIVES (HSPDs) AND THEIR EFFECT ON THE SECURITY INDUSTRY

TABLE OF CONTENTS:

I. INTRODUCTION

Due to the rapidly changing landscape of Federal Government security requirements and in an effort to prepare our industry sector for the inevitable changes that will apply to their products in the very near future, this is a special report on Homeland Security Presidential Directives (HSPD), their immediate effects and possible future effects on industry. The QTU subject scheduled for this quarter, *Authentication, Authorization and Encryption*, will be addressed in the Q3 QTU.

This report will specifically look at the requirements for HSPD[1] 5, 7, 8 and 12 in the order that they will be felt by industry. Therefore we will review HSPD-12, HSPDs 5 and 8 and finally HSPD-7 in that order.

A key concept of this QTU is that US Government automated security, access control and digital video systems are now considered Information Technology (IT) systems, and as such, all of the protections and design criteria applicable to IT systems in the Federal space will be applicable to these systems. One significant overarching requirement that has emerged within government is interoperability, stated originally in the USA Patriot Act as the ability for data to be "cross agency and cross platform compatible". Remember that individual agencies will deter-

mine applicable criteria, so there may be some latitude in the initial phases, specifically with regard to digital video. This will require those choosing to do business with government to develop products that are based on an open architecture and that are easily integrate-able, compatible, document-able and scalable. Furthermore, any non-governmental agency purchasing equipment with Federal grant monies will most likely be required to comply with these requirements as well. This amounts to a sizeable incentive for change.

Consider a definition from FIPS 191, *Guideline for The Analysis [of] Local Area Network Security,* "The Institute of Electrical and Electronic Engineers (IEEE) has defined a Local Area network (LAN) as "a datacomm system allowing a number of independent devices to communicate directly with each other, within a moderately sized geographic area over a physical communications channel of moderate rates" [MART89]. Typically, a LAN is owned, operated, and managed locally rather than by a common carrier. A LAN usually, through a common network operating system, connects servers, workstations, printers, and mass storage devices, enabling users to share the resources and functionality provided by a LAN."[2] Clearly many of the security industry product offerings fall within this definition.

If you plan to do business with the Federal Government, it is recommended that you review FIPS Publication 199[3], *Standards for Security Categorization of Federal Information and Information Systems.* From Section 2, "These standards shall apply to: (i) all information within the federal government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status; and (ii) all federal information systems other than those information systems designated as national security systems as defined in 44 United States Code Section 3542(b)(2). Agency officials shall use the security categorizations described in FIPS Publication 199 whenever there is a federal requirement to provide such a categorization of information or information systems." As our systems converge into the Federal IT space's categorization of security information and information systems, they will be subject to the applicable Federal IT security rules and standards.

In the context of this QTU, HSPD 5 and 8 will be analyzed as they apply to the "first responder" community, State and local facilities and other "critical infrastructure" physical electronic security equipment upgrades and acquisitions. Although most SIA member companies are not heavily vested in the first responder market, in-car video systems will definitely be affected. The need for situational awareness at the scene of an incident may impose future requirements on video systems as evidenced in the Next Generation Aviation Transportation Systems[4] (NGATS) implement-able by 2025 where law enforcement first responders are envisioned as having the ability to receive live wireless video feeds from an airport's video surveillance systems if and when needed. At least one school district is currently documenting the interior of their schools with 360 degree digital cameras as part of a future response plan to incidents similar to Columbine. This detailed mapping, as well as access to live video feeds,

is envisioned as key resources for first responders in the future to these types of incidents.

HSPD-5 further mandates the creation of the National Incident Management System[5] (NIMS) and we will be looking specifically at Chapter VI of the NIMS, *Supporting Technologies.* HSPD-5 also mandates the creation of the National Response Plan[6] (NRP) which in turn implements the NIMS. HSPD-8 is a companion document to HSPD-5. It expands upon the requirements of HSPD-5 and will be reviewed jointly with HSPD-5.

HSPD-7 deals with Critical Infrastructure Identification, Prioritization, and Protection. HSPD-7 spawned the *2004 National Critical Infrastructure Protection Research and Development Plan*[7] signed on 8 April 2005. Taken from the NCIP R&D "The December 17, 2003 Homeland Security Presidential Directive - 7 (HSPD-7) established a national policy for federal departments and agencies to identify and prioritize United States critical infrastructures and key resources, and to protect them from terrorist attacks. Further, it established a policy to prepare a national critical infrastructure protection (CIP) research and development (R&D) plan to provide the sustained science, engineering, and technology base needed to prevent or minimize the impact of future attacks on our physical and cyber infrastructure systems. This document provides the R&D plan required by this Presidential Directive." The NCIP R&D holds out the hope of improved, new and novel applications of technologies that will be developed for perimeter detection sensors (among other technologies) and will be directly transferable to industry. This is the bright spot of the HSPDs for industry.

HSPD-12 has been a priority for SIA members and is the most pressing HSPD from a time compliance perspective. Let's start with it.

II. HSPD-12

Our industry has known for some time that the convergence of electronic physical security systems and the IT sector has been imminent. Past conversations with manufacturers indicated that the generally accepted time frame for this convergence was within five to ten years. The reality is that by 27 October of 2005 all Government agencies must have a process in place to issue Smart Card based credentials. Beginning on this date they will begin to implement that process. Draft OMB guidance[8] indicates that by October 2006, the Federal Government will begin to issue an estimated 15 million Smart Cards. These deployments must be completed by a date approved by the Office of Management and Budget (OMB), still forthcoming. Soon thereafter, access to all information systems and government facilities in the Federal space will require a FIPS 201[9], PIV-2 compliant credential that will include biometric fingerprints and Federal Bridge Public Key Infrastructure (PKI) certificates and digital signatures. Most integrated access control and video systems (within the Government) will use the Federal Bridge PKI for both system administration and user operation. As a reminder, these systems will need to be Certified and Accredited in accordance with Special Publication (SP) 800-37[10]. This Certification and Accreditation requirement can be viewed as an opportunity by member companies to develop contacts within government and to familiarize them with the unique features inherent to each system.

Finally, each system must under go a Privacy Impact Assessment (PIA).[11] Agencies are required to conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available. Once again, this will require manufacturers to fully understand the extent of their equipments protections and be able to effectively communicate same in the context of a PIA, once again a great sales lead-in.

Due to privacy concerns, the Federal Smart Card will contain two distinct interfaces. This can take the form of two Integrated Circuit Chips (ICCs), or a single dual interface chip if it is capable recognizing which interface is being employed and allow access to data consistent with what is allowed for that interface. One interface will be a "contact" interface requiring physical contact with the reader. This chip, or compartment on the dual interface chip, will contain all personal or sensitive information such as biometrics template, cardholder name, DOB, etc. and will be powered by direct contact with the reader. This will be used for logical access to IT assets in the Federal space. The other will be a "contact-less" interface and will contain limited, non-readily identifiable information. This will be a *close range* contact-less interface.

The current envisioned scenario is that initial authentication and authorization into a local Physical Access Control System (PACS) will be accomplished using the "contact" side of a Smart Card with the cardholder providing a Personal Identification Number (PIN) and biometric for user authentication and identity verification. Once enrolled in the local PACS, the "contact-less" side of the Smart Card will be used in an effort to emulate current throughput capabilities of proximity reader enabled PAC Systems (i.e. 400 milliseconds maximum per transaction) at major choke points. The contact-less chip will contain the Cardholder Unique Identifier, or CHUID, and a component of this number, the Federal Agency Smart Credential Number, or FASC-N, will be used as an identifier for the cardholder in a manner consistent with current proximity reader enabled systems. The main thing to remember is that the FASC-N must be unique in a "campus" that is now comprised of all U.S. government facilities, worldwide. The FASC-N as defined in NIST Special Publication 800-73[12] is a 25 byte number. The Government is considering the resurrection of FIPS 95-2, Federal Agency Smart Credential Number (FASC-N). These U.S. Government agency codes are available in the old FIPS 95-2[13].

In a very real way, the traditional 26 bit Wiegand protocol has met its end in the Federal space. Readers that are to be used for FIPS 201 compliant systems must be ISO[14] 7816 compliant for the "contact" side of the card and ISO 14443 compliant for the "contact-less" side of the card.

This forced timeline applies to the Federal space only, but as mentioned before, large end users almost invariably follow suit. Remember that any Federal funds used to purchase equipment for state and local government or first responder needs (local government buildings, police stations, firehouses, etc.) must also comply with interoperability and compatibility criteria due to guidelines set forth in the National Incident Management System (AKA the NIMS, reviewed later in this document). The most likely scenario will be that the NIST SP 800-73 and SP 800-76 requirements will be applicable to these systems as

well, allowing for seamless interoperability between Federal, State, local government and first responder credentials (see next paragraph) and systems in the event of an "incident". Essentially HSPD-12 has dictated the timetable for the evolution of our industry. This is because although access control is taking the brunt of this forced evolution, digital video systems in the Federal space will also be required to be accessed using Smart Card technologies with a Federal Bridge PKI certificates and digital signatures for authentication and authorization. Furthermore, all IT system (and PACS as well as Digital Video Systems are now considered IT by government) architecture will have to be open. This means that in the very near future ALL physical electronic access control and digital video systems will be open architecture and interoperable or Federal funds will not be available for their purchase, **period**.

Although not mandated by HSPD-12, there is currently discussion in the Federal Government to provide first responders with a Smart Card based credential that would allow chain of command at an incident the ability to scan the credential with a reader (hand held or networked) to verify that the bearer is who they claim to be. This credential would also document the bearers unique qualifications as they apply to the incident. This would allow for an inventory of specialized knowledge and skills available to command at the site of an incident. Once again, these systems are envisioned as being purchased with Federal funding and subject to NIMS requirements.

To recap, the essence of HSPD-12 is (from an equipment point of view only):

- The Credential will be reliable and secure.
- The Credential and Systems provisioning and processing it must be interoperable.

III. HSPDs 5 & 8

HSPD-5[15] targets the unified response to an incident[16]. Its purpose is defined in HSPD-5 as "To enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system." Paragraph 15 of HSPD-5 specifically charges the Secretary of Homeland Security with the creation of a National Incident Management System, or NIMS. We will look at the NIMS a little later in more detail. Paragraph 16 charges the Secretary of Homeland Security with developing the National Response Plan, or NRP. From paragraph 16(a) "The NRP, using the NIMS, shall, with regard to response to domestic incidents, provide the structure and mechanisms for national level policy and operational direction for Federal support to State and local incident managers and for exercising direct Federal authorities and responsibilities, as appropriate." Paragraph 20 (bold type by author) states "**Beginning in Fiscal Year 2005**, Federal departments and agencies shall make adoption of the NIMS a requirement, to the extent permitted by law, **for providing Federal preparedness assistance through grants, contracts, or other activities**. The Secretary shall develop standards and guidelines for determining whether a State or local entity has adopted the NIMS." So it is clear that the NIMS is the source for direction for State, local and first responder equipment requirements in order to be eligible for Federal grant monies for purchase. The grant monies available through the Homeland Security Grant Program[17] for FY 2005 is three billion dollars "for planning, equipment, training, exercises, and program management and administration for

emergency prevention, preparedness, and response personnel in all 50 states, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories, while expanding the scope and reach of the program."

These grants have been mandated by HSPD-8[18]. The purpose of HSPD-8 is quoted as "establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal[19], establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities." From paragraph 8: "Full implementation of a closely coordinated interagency grant process will be completed by September 30, 2005." But one of the most important paragraphs as it applies to the use of grant monies for equipment purchases by State and local authorities and first responders is paragraph 14:

"Federal preparedness assistance will support State and local entities' efforts including planning, training, exercises, interoperability, and equipment acquisition for major events as well as capacity building for prevention activities such as information gathering, detection, deterrence, and collaboration related to terrorist attacks. Such assistance is not primarily intended to support existing capacity to address normal local first responder operations, but to build capacity to address major events, especially terrorism." Entities requesting grant monies, or "preparedness funding", must be NIMS compliant[20]. This can be interpreted as a good thing for our industry as old and outdated access control, intrusion detection and video systems are replaced or fortified and new systems installed in and around critical infrastructure including State and local government buildings, police and fire stations, power generation and transmission facilities, transportation and internet infrastructure and medical facilities. It is prudent to look at the NIMS for guidance on equipment requirements.

The NIMS provides a "consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among Federal, State and local capabilities, the NIMS will include a core set of concepts, principles, terminology, and technologies covering the incident command systems; multiagency coordination systems: unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications and certifications; and the collection, tracking, and reporting of incident information and incident resources." The requirements for "interoperability and compatibility" are plainly stated in the scope.

Chapter VI, *Supporting Technologies*, section A, *Concepts and Principles*, number 1, *Interoperability and Compatibility*, (VI.A.1) reads, " Systems must be able to work together and should not interfere with one another if the multiple jurisdictions, organizations and functions that come together under the NIMS are to be effective in domestic incident management. Interoperability and compatibility are achieved through the use of such tools as common communications and data standards,

digital data formats, equipment standards, and design standards."

How will this requirement affect the security industry? As our industry moves down the road towards interoperability through the efforts of the SIA Standards Department, industry should be well positioned to comply with this overarching requirement. Standards compliance is voluntary, and it will be the choice of individual member companies to build equipment that complies with the Standards, but at least industry will have access to a body of standards that address this critical issue.

Manufacturers of in-car video systems used by law enforcement agencies are not as fortunate. It is estimated that 80% of these systems are purchased with Federal grant monies; fully 100% of the digital systems manufactured by approximately 65 in-car video manufacturers are proprietary. For this niche industry sector to continue to receive orders from police departments funded by Federal monies, they will have to agree upon a common "digital data format" to be used by the entire industry as well as migrate to an open architecture back-end system for storing, archiving and retrieval of video clips. This will allow incident scene video images captured on in-car systems to be made available to incident command as well as allow images to be shared by disparate Federal, local and State police departments as well as the intelligence community. This could be invaluable in apprehending suspects from an incident scene or understanding the cause of the incident.

Furthermore, in-vehicle components will most likely be required to be interoperable using standardized interfaces and connectors allowing for the retrieval of the recording device in situations where the vehicle is disabled, allowing for play back on another vehicles system (possibly a vehicle from another jurisdiction). This will insure timely access to potentially critical information about an incident scene.

Another major concept in the NIMS is reflected in Chapter VI.A.3. In part, "National Standards for key systems may be required to facilitate the interoperability and compatibility of major systems across jurisdictional, geographical and functional lines." This is further expanded on in section VI.2. It is obvious from section VI.2 that performance metric standards rank as highly as interoperability and compatibility for any equipment used by incident management teams.

HSPD-5 and 8 will affect industry in the foreseeable future, not only for companies that decide to serve the Federal government, but for anybody deciding to bid on critical infrastructure protective systems where those funds are Federal monies.

To recap, the essence of HSPD-5 and HSPD-8 are:

- Establishes the NIMS and NRP.
- There will be unified incident response and management.
- Equipment will be interoperable and compatible.
- Equipment performance metric standards will apply.
- Federal monies will be made available to facilitate these goals.

IV. HSPD-7

The purpose of HSPD-7 is stated as "establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks." As noted in the introduction of this QTU, HSPD-7 is also the basis for the 2004 *National Critical Infrastructure Protection Research and Development Plan* which was signed by Michael Chertoff, Secretary of Homeland Security and John H. Marburger, III, Director, Office of Science and Technology Policy, on 8 April 2005. The *NCIP R&D Plan* will be reviewed and updated annually, but the 2004 *NCIP R&D Plan* serves as a baseline. The *NCIP R&D Plan* is "structured around nine science, engineering, and technology themes that support all critical infrastructure sectors, encompass both cyber and physical concerns, and are strongly integrated in a layered security strategy. The themes are:

- Detection and Sensor Systems;
- Protection and Prevention;
- Entry and Access Portals;
- Insider Threats;
- Analysis and Decision Support Systems;
- Response, Recovery, and Reconstitution;
- New and Emerging Threats and Vulnerabilities;
- Advanced Infrastructure Architectures and Systems Design;
- Human and Social Issues."

Additionally, "The long-term vision of the CIP R&D plan involves three strategic goals. These drive the requirements in the *NCIP R&D* to assure the future security of the Nation's critical infrastructure and include:

- A national common operating picture for critical infrastructure.
- A next-generation computing and communications network with security "designed-in" and inherent in all elements rather than added after fact.
- Resilient, self-diagnosing, and selfhealing physical and cyber infrastructure systems."

One priority is "*Improve Sensor Performance* – Develop improved physical and cyber monitoring and detection systems that will include enhancements in speed, fewer false-positive readings, reduced power requirements, increased durability, and lower cost. These sensors will have increased sensitivity, be environmentally aware, have higher accuracy, and include both active and passive sensors and robotic platforms."

Another identified priority is to advance "Risk Modeling, Simulation, and Analysis for Decision Support". The SIA Standard's Program is contributing to this aspect by developing performance metric standards that will allow quantification of a sensor's performance for input into mathematical risk analysis and mitigation models. One example of such a Standard is the Draft SIA PIR-02 standard that should be published in Q1 2006.

The 2004 *Plan* will serve as both a baseline and vision document of needs for the country's critical infrastructure. From the 2004 Plan "With a baseline in place and a vision identified, an **investment plan** can be developed in the **2005 NCIP R&D** planning effort. Future plans will place more emphasis on the identification both of development efforts that could provide near-term protection and of science and technology efforts that are longer-

term and more speculative but that could provide inherently secure or systemic approaches to the sharp reduction of vulnerabilities."

This should provide for both short and long term funding for technologies that can be leveraged by industry. To recap, HSPD-7 strives to:
Create a baseline of efforts and technologies. Will be revised annually.
Provides for the development and enhancement of technologies through funding.

V. CONCLUSION

The HSPDs we have reviewed have just been lightly mined for pertinent data and deserve in depth investigation by affected parties. It is clear that industry is feeling the impact of these Directives and will continue to feel this impact for years to come. Our industry has evolved significantly over the past five years. This is nothing compared to the degree of evolution that will take place over the next two to three years. Proprietary solutions are no longer acceptable to one of the largest end users, the U.S. Government, and they have leveraged there weight by requiring any purchases for State, local and first responder equipment to be compliant with the NIMS requirements. Access control is taking the point position on the road to IT-security convergence, with digital video close on its heels.

There is a strong need for standards for both interoperability as well as performance metrics cited in many of the documents discussed in this QTU. There have also been mechanisms delineated to help produce those standards and there will be funding sources to help these in the future.

Welcome to the integrated future, we no longer have a choice.

FOOTNOTES

[1] Homeland Security Presidential Directives can be viewed here: http://www.whitehouse.gov/

[2] FIPS 191 can be downloaded here: http://csrc.nist.gov/publications/fips/fips191/fips191.pdf

[3] FIPS 199 can be downloaded here: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[4] NGATS: http://www.jpdo.aero/site_content/NGATS_v1_1204.pdf see Chapter 4.1

[5] The National Incident Management System can be downloaded here: http://www.fema.gov/pdf/nims/nims_doc_full.pdf

[6] The National Response Plan can be downloaded here: http://www.dhs.gov/interweb/assetlibrary/NRP_FullText.pdf

[7] The National Critical Infrastructure Protection Research and Development Plan can be downloaded here: http://www.dhs.gov/interweb/assetlibrary/ST_2004_NCIP_RD_PlanFINALApr05.pdf

[8] The official OMB guideline has not been issued yet and this timeline ***may*** be subject to change.

[9] FIPS-201 can be downloaded here: http://csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf

[10] SP 800-37 as well as any other NIST Special Publications can be downloaded here: http://csrc.nist.gov/publications/nistpubs/index.html

[1] See OMB Circular M-03-22: http://www.whitehouse.gov/omb/memoranda/m03-22.html#a

FOOTNOTES {CONTINUED}

[12] NIST SP 800-73 page 46, second table. SP 800-73 is available at: http://csrc.nist.gov/publications/nistpubs/800-73/SP800-73-Final.pdf

[13] FIPS 95-2 can be downloaded here: http://niatec.isu.edu/pdf/new/fips95-2.pdf

[14] ISO- International Organization for Standardization: http://www.iso.org/iso/en/ISOOnline.frontpage

[15] HSPD-5 can be viewed here: http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html

[16] An "incident" is defined in HSPD-5 as "terrorist attacks, major disasters, and other emergencies".

[17] The Homeland security Grant Program FY 2005: http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf

[18] HSPD-8 can be viewed here: http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html

[19] Information on the National Preparedness Goal can be viewed here: http://www.ojp.usdoj.gov/odp/docs/Goal_041305.pdf

[20] For more information on NIMS compliance, go here: http://www.nimsonline.com/