Global Information Assurance Certification Paper

SANS Institute – GIAC Security Essentials Certification (GSEC)

Practical Assignment – Version 1.4b, Option 1

Submitted by Carla Dancy Smith

Crosswalking Security Requirements

Monday, March 8, 2004

Table of Contents

I. Abstract

This paper provides the background and the steps for conducting a policy focused security requirements crosswalk or mapping. This discussion is geared towards Chief Information Officers (CIOs), and others trying to navigate the road to security compliance. The Meridian Dictionary defines crosswalk as a "specially paved or marked patch for a pedestrian crossing a street or road." Unfortunately, there is no specially paved road or marked path to walk on the street toward compliance with security regulations. Following this analogy, there are in fact, many security regulations (roads), and no single security standard (path); and there is no one map leading from Point A to Point B. CIOs are faced daily with the daunting challenge to secure their networks, workplaces, data, inventories, and all aspects of their operations in accordance with many different security regulations, as dictated by various industry and government defined security standards. CIOs, and others responsible for ensuring compliance with the applicable security requirements, without a map in hand, probably often ask themselves:

- Where to begin on the road towards security compliance?
- Which security regulations to implement first?
- What security standards are best practices?

The paper provides a discussion of how performing a security requirements crosswalk analysis can help a CIO, or a novice, to answer these questions. The paper includes an illustrative approach to conducting a crosswalk of security requirements focused on the healthcare sector, and specifically the Health Insurance Portability and Accountability Act (HIPAA). It includes the steps in a security crosswalk process and a sample crosswalk template. Senior executives acknowledge that non-compliance, or the failure to implement the proper security safeguards, can result in loss or damage to valuable assets; including but not limited to: competitive or proprietary data; customer information; personnel resources; credibility and brand; protected health information – and ultimately - productivity, time and money. Therefore, continuing the analogy, a security requirements crosswalk is not just a leisure stroll in the park, an intellectual analysis done for the sake of curiosity or academic study. But rather, a security requirements crosswalk is a critical and valuable tool, a calculated and measured stride down a specially paved road toward the desired destination termed compliance. The results of a non-technical security requirements crosswalk can lead to a greater understanding as to how to comply with many security requirements in the absence of one security standard, by leveraging existing security practices already in place within an organization.

II. Background

Even before the events of 9/11 caused the current shift in national priorities to homeland security issues, there was an understanding by most CIOs that our nation's critical infrastructure needed protecting, that there are efficiencies to be gained by sharing more data electronically among government agencies, and that citizens wanted to conduct business through e-commerce with the government as they had grown accustomed to doing with corporations. In order to accomplish these information technology driven functions, the U.S. government had passed a patchwork of legislation and implemented a web of regulations and decisions concerning how security issues were addressed in the public and private sector. At the highest level, these security mandates, individually, were designed to address the problems that surfaced as business and government moved from the industrial age, to the information age, and then to the knowledge or "Internet" era. Collectively, these security mandates are suppose to offer structure to the fast-paced new world order where services and ideas are as critical as products, and global instantaneous communications is the norm. In the twenty-first century economy, electronic networks are the backbone and increasingly the primary vehicle for business and government operations. Information technology policy is now the hot topic imbedded in and across all sectors and issues, and security is an integral part of this equation.

A. Security Related Legislation

The most significant legislation affecting the security practices of government agencies include, but are not limited to (Note: All of the URLs for the sources below are listed in the References Section of this paper): [1]

SELECTED LEGISLATION	SUMMARY
Government Performance and Results Act (GPRA)	• Requires agencies to prepare multi-year strategic plans that describe their agency goals and action plan for achieving, including information technology related topics • Designed to ensure that results are tied to a budget
Government Paperwork Elimination Act (GPEA)	• Calls for Federal agencies to offer digital forms and accept electronic signatures • Requires agencies to give the public, businesses and other agencies the option of submitting information electronically • Mandates the use and acceptance of electronic signatures to bind such transactions
Government Information Security Reform Act	• Addresses the program management, evaluation and reporting aspect of Federal information technology security and establishes and oversight process • GISRA replaced by FISMA
Gramm-Leach-Bliley Act	• Requires Federal agencies and states to prepare cyber security guidance for financial institutions

Selected Legislation	Summary
Sarbanes-Oxley Act	• Requires more stringent financial reporting and auditing guidelines on public companies • Encourages the implementation of an internal compliance-oriented infrastructure, with adequate security controls, to reduce fraud and abuse and to facilitate the required accurate financial reporting
Clinger-Cohen Act of 1996	• Established an Information Technology Investment Management framework • Updated the model recently to include five stages of investment management maturity
Health Insurance Portability and Accountability Act (HIPAA)*	• Includes a Security Rule that includes procedures for protecting electronically transmitted personal patient health and medical data
E-Government Act of 2002	• Establishes enterprise architecture and other standards • Requires Federal agencies to complete a Privacy Impact Assessment (PIA) which requires IT or privacy professionals to assess whether appropriate privacy policies, procedures, and business practices – as well as applicable administrative, technical, and physical security controls – have been implemented.
Federal Information Security Management Act of 2002 (FISMA)	• Includes a section on information security requiring program management, evaluation, and reporting activities • Establishes a framework for ensuring effectiveness of Federal information security controls along with guidance regarding the development and maintenance of minimum standards

*For purposes of the security requirements crosswalk in Section IV of this document, the HIPAA Security Rule will be the selected legislation considered, or the driver of the analysis. However, a crosswalk can be conducted using any selected legislation.

The paper focuses mostly on the security requirements mandated for government agencies, but there is incidental applicability to the private sector. In the context of this paper, as defined in FISMA, "information security'" means "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction." Each of these regulatory requirements includes guidance that touches to some degree information technology systems, information security, security systems, and/or ultimately security standards.

The above list of Federal mandates is not exhaustive, as it omits many pertinent security related guidance documents issued by the White House Office of Management and Budget (OMB). The OMB memorandum are often issued as announcements, clarifications or in response to questions raised about regulations. The enforcement entity for the Federal mandates varies; but it can be OMB, or the Federal judicial system, the HHS Office of Civil Rights (in the case of HIPAA) or the Federal Trade Commission, an agency's own Inspector general (IG) or other source.

These above information security related regulations are at varying stages of implementation, oversight and performance review across government agencies, and the private sector. In some cases, the Congress and the Federal agencies responsible for adopting and implementing security regulations are considering amendments and revisions to current security regulations, as there is still not perfection in this realm. Keeping track of security related legislation and the implications for Federal agency policy, procedures and practices is only one responsibility of the CIO.

B. Security Related Standards

Security standards are the technical means by which an organization intends to implement and manage the security of its information to meet the objectives and goals established in the legislation, regulations and guidance described above. Security standards usually address management, operational, technical and physical areas where more detailed actions must be taken to conduct security reviews. Implementing security standards involved management decisions regarding the level of risk an organization wishes to accept and its risk mitigation strategy.

With regards to security standards, self-regulation by industry is common, and often preferred by the private sector; for fear that the issuance of government security standards or requirements may stifle competitive forces or inadvertently preference one technology over another. Depending on the sector, whether a business is national or international, whether an agency is Civil, Defense, or Intelligence, and other characteristics of its operations, some of the most widely recognized security standards, one process and one tool are described in the table below: (Note: All of the URLs for the sources below are listed in the References Section of this paper): [2]

SELECTED SECURITY STANDARDS	SUMMARY
National Institute of Standards and Technology (NIST) 800 Series Publications	• "Under the Computer Security Act of 1987 (P.L. 100-235), the Computer Security Division of the Information Technology Laboratory (ITL) develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. These publications present the results of NIST studies, investigations, and research on information technology security issues. • The publications are issued as Special Publications (Spec. Pubs.), NISTIRs (Internal Reports), and ITL (formerly CSL) Bulletins. Special Publications series include the Spec. Pub. 500 series (Information Technology) and the Spec. Pub. 800 series (Computer Security). Computer security-related Federal Information Processing Standards (FIPS) are also included." • Under FISMA provisions will develop standards to be used by the Federal agencies to categorize information and information systems; will develop guidelines for identification of national security information and information systems and related categories and information security requirements.

SELECTED SECURITY STANDARDS	SUMMARY
Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)*	• A process that applies to all services, components, activities and their contractors or agents • "Establishes a standard DoD-wide process, set of activities, general tasks, and a management structure to certify and accredit management Information Systems (IS) that will maintain the Information Assurance (IA) and security posture of the Defense Information Infrastructure (DII) throughout the lifecycle of the system." • Policies are set out in DoD 8510.1-M; derived from DoD Directive 8500.1, Information Assurance. • A *process* which implements policy, assigns responsibilities and prescribes procedures for certification and accreditation of information systems, including information systems, networks, and sites in DoD. • The foundational document of the DITSCAP is the System Security Authorization Agreement (SSAA), which is used throughout the DITSCAP to guide actions, document decisions, specify IA requirements, document certification tailoring and level of effort, identify potential solutions, and maintain operational systems security."
DoD Directives	• There are numerous other DoD specific security related directives and regulations, including, but not limited to: 1. DoD Directive 5000.1, defense Acquisition 2. DoD Directive 5000.1.R, Information Security Program 3. DoD Directive 5200.28-STD, Trusted Computer System Evaluation
OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation℠)	• "A tool designed for an organization that wants to understand its information security needs • A risk-based strategic assessment and planning technique for security"
American National Standards Institute (ANSI)	• "A private, non-profit organization (501(c)3) that administers and coordinates the U.S. voluntary standardization and conformity assessment system. • The Institute's mission is to enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity. • Although ANSI itself does not develop American National Standards (ANSs), it provides all interested U.S. parties with a neutral venue to come together and work towards common agreements." • Security is an ancillary issue, not the primary standard addressed by this group
International Organization for Standardization (ISO) 17799	• "Detailed security standard organized into ten major sections, each covering a different topic or area: 1. Business Continuity Planning 2. System Access Control 3. System Development and Maintenance 4. Physical and Environmental Security 5. Compliance 6. Personnel Security 7. Security Organization 8. Computer & Operations Management 9. Asset Classification and Control 10. Security Policy • Within each section are the detailed statements that comprise the standard."

SELECTED SECURITY STANDARDS	SUMMARY
International Electrotechnical Commission (IEC)	• "The leading global organization that prepares and publishes international standards for all electrical, electronic and related technologies. These serve as a basis for national standardization and as references when drafting international tenders and contracts." • Security is an ancillary issue, not the primary standard addressed by this group
System Security Engineering Capability and Maturity Model (SSE CMM)	• The SSE CMM Model "describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering."

*For purposes of the security requirements crosswalk in Section IV of this document, DITSCAP will be the selected security standard process considered, or the subject of the comparison with the HIPAA Security Rule. However, a crosswalk can be conducted using any selected security standard.

The CIO and/or others responsible for security requirements implementation must be current in their understanding as to the security standards that are applicable in the environment, as well as for new and emerging technologies, such as wireless. The crosswalking of security requirements may be useful in mapping the requirements that come from these multiple sources to see where duplication and redundancies exisit.

III. Security Requirements in the Healthcare Sector

From a historical perspective, the concept of protecting information is a long established ethical code in the healthcare environment. Traditionally, physicians are bound by the Hippocratic Oath, which establishes that what is seen or heard during the course of treatment is to be kept to oneself. The classical translated version of this Hippocratic Oath states that: "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about." [3]

There are other concepts in the Hippocratic Oath that are being debated as to their relevance and applicability in the realm of modern medicine. [4] But the protection of patient information principal seems to have endured the test of time, and is included in modern codes of ethics as promoted by the American Medical Association (AMA) and other similar professional societies. [5] Keeping this oath is still an underlying theme in the medical profession.

The principal of confidentiality, which security controls protect, is even more critical in the age of prolific paper-based systems that are moving quickly towards electronic medical records. The new healthcare environment also has an increased deployment of mobile medical devices, web-enabled home health monitoring instrumentation, wireless functionality, integrated and networked hospital facilities, doctors' practices, pharmacies and so forth all of which need securing and protecting by all of the involved medical professionals as well as the healthcare sector based CIOs.

Meeting standards or requirements is not a new concept for the healthcare management team. For example, hospitals must obtain periodic certifications; medical equipment must meet the Federal Drug Administration (FDA) testing standards before deployment; pharmaceutical drugs must pass clinical trials before they are marketed to the general public; doctors and nurses must obtain credentials in order to pursue their professions; and sanitary conditions have to be maintained in the health delivery environment.

It is in this complex environment that the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) came to be law. HIPAA requires "the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data. Adopting these standards will improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in health care."[6]

As covered entities struggle to comply with the HIPAA Final Security rule that becomes effective on April 5, 2005, [7] one of the first questions asked is: "What security practices are presently in place in the organization that may help in meeting the security requirements dictated in HIPAA?" All healthcare organizations must/should have some security measures in operation in accordance with sound business practices. The extent of these measures usually varies based on the size, location, mission, function, and other factors related to a healthcare entity. HIPAA is the current driver for more closely examining and evaluating the current security procedures, polices, processes, and protections and determining their adequacy toward complying with the HIPAA Final Security Rule.

There is however an underlying potential conflict in the healthcare setting as two of the main actors have different primary motivations. The healthcare professional is most concerned with "saving lives" and "delivering medical services." The security professional is focused on "protecting and securing computer systems and the associated information."

Ideally and ultimately, organizations trust that both the medical and security staff is committed to the higher mission of the Federal agency or corporation. This mission will hopefully be their common bond that will facilitate collaboration on the security issues and wellness in the healthcare environment. At the end of the day, the patient, as well as all other stakeholders, must care, and insist, that the medical, security, and overall mission objectives are achieved, because they are intimately interconnected, not mutually exclusive, and can be a matter of life and death in today's networked healthcare setting.

Recognizing that security related standards are a relatively new concept for the healthcare professional to adapt, it is important to marry the healthcare workers' traditional standards associated with "saving lives," with those standards associated with "security functions." Any relief, or process, to ease the pain in implementing these new security related requirements being placed upon an already overburdened, resource constrained healthcare industry would logically be welcomed.

For the CIO, a security requirements crosswalk may offer such relief, as it is designed to build upon and maximize the existing security processes and procedures in place while complying with new security related regulations, such as HIPAA. Depending on the environment, there are potentially several other health care specific requirements and accreditations that a health related entity is already in gear to meet even prior to HIPAA becoming law, such as, but not limited to: (Note: All of the URLs for the sources below are listed in the References Section of this paper) [8]

SELECTED HEALTHCARE SECTOR STANDARDS AND ACCREDITATIONS*	SUMMARY
The Joint Commission on Accreditation of Healthcare Organizations (JCAHO)	• Evaluates medical facility compliance based on a focused set of "requirements" that are long known as essential to the delivery of good patient care
CMS Core Security Requirements (CMS CSR)	• "Detail technical requirements for business partners who use IT systems to process Medicare data. Business partners must establish and maintain responsible and appropriate controls to ensure the confidentiality, integrity, and availability of Medicare data. CMS has organized the Core Security Requirements into Categories, General Requirements, Control Techniques, and Protocols. There are ten Categories 1. Entity-wide Security Program Planning and Management Elements 2. Access Control 3. System Software 4. Segregation of Duties 5. Service Continuity 6. Application Software Development and Change Control 7. Application System Authorization Controls 8. Application System Completeness Controls 9. Application System Accuracy Controls 10. Networks"

SELECTED HEALTHCARE SECTOR STANDARDS AND ACCREDITATIONS*	SUMMARY
CMS Internet Security Policy	• Issued in 1998 by then named Health Care Finance Association (HCFA), it "established the basic security requirements that must be addressed for use of the Internet to transmit HCFA Privacy Act protected and/or other sensitive HCFA information." This bulletin remains in effect until canceled or superceded.
URAC Information Security	• "Offers a Security Audit service that will aid health care organizations in developing and maintaining an information security protection strategy. • Takes a comprehensive look at how organizations are dealing with a wide range of security risks within their operations, and offer recommendations for improvement to help meet the expanding number of security-based regulatory and business requirements in the health care field."
NCQA Certification and Accreditation Standards	• "An independent, 501(c)(3) non-profit organization whose mission is to improve health care quality everywhere. • NCQA evaluates health care in three different ways: through accreditation (a rigorous on-site review of key clinical and administrative processes); through the Health Plan Employer Data and Information Set (HEDIS® -- a tool used to measure performance in key areas like immunization and mammography screening rates); and through a comprehensive member satisfaction survey. Although participation in our accreditation and certification programs is voluntary, more than half the nation's HMOs currently participate. And almost 90 percent of all health plans measure their performance using HEDIS."

*Though not illustrated in this paper, the above healthcare sector specific standards could also be considered for a crosswalk analysis. Even though these standards are not focused on security, they may have elements that touch security related topics.

The list above is only a representative sample of some recognized healthcare specific regulations. It is worth exploring the degree to which these regulations, or any others being implemented within a healthcare entity, include security related provisions that can be built upon and leveraged to meet any new security requirements, dictated in new laws like the HIPAA Security Rule. Achieving economies of scale in the area of security, eliminating duplicative efforts and documentation, achieving efficiencies, all in cost effective manner, but yet fully complying with all security mandates is the goal. A security requirements crosswalk can assist with this endeavor.

IV. Security Requirements Crosswalk Methodology

Admittedly, the security crosswalk methodology outlined here is but one recommended approach. This crosswalk methodology is purposefully present in as non-technical manner and in as simplistic terms as possible so that it may be embraced by non-security experts, including healthcare professionals.

A more technical similar exercise may be called a security requirements traceability matrix (SRTM). A SRTM "focuses on understanding the information system requirements, the environment in which the information system will operate, the uses of the information system, the security requirements that apply to the information system, and the level of effort necessary to achieve certification. The objective of a SRTM is to agree on the intended system mission, security requirements, schedule, and resources required for the certification effort." [9]

This security requirements crosswalk is a similar process but a little less formal and technical. The end objective for the crosswalk is not systems certification but an understanding of what is required to achieve compliance. The crosswalk has eight basic steps described in some detail in this section:

A. Select the standards for the crosswalk exercise

The methodology for conducing a security requirements crosswalk below is focused in the healthcare environment, using HIPAA Security Rule as the anchor regulation, or driver. However, this methodology can be used for crosswalking any chosen security requirements, standards, processes and/or tools. Crosswalking can be helpful in recognizing gaps in the current operations with the ideal or required state.

B. Define crosswalk assumptions, disclaimers, and parameters

It is critical to manage the expectations as to the outcomes and applicability of the results of the crosswalk exercise. Merely completing a crosswalk, where elements of both security standards are found to overlap does not mean an organization is compliant. Terms to describe the degree of potential "satisfaction of a security standards requirement" need to be carefully defined, understood and agreed at the onset. The following is a list of some assumptions topics to be considered:

- Explain the level of analysis, degree of real-world verification of the activities described in the standards being compared.
  Example: The analysis is theoretical and high-level. Or conversely, on-site interviews will be conducted to determine the degree to which the standards are being followed.
- Set expectations clearly.
  Example: An in-depth gap analysis of the structures and business relationships within the organization as it relates to these interconnecting security requirements may produce more program specific compliance guidance.

- Define the limitations of the analysis.
  Example: HIPAA compliance will not substitute or negate the requirement for compliance with other regulations and policies, and vice versa.
- Explain potential compliance constraints
  Example: The DITSCAP process, if properly followed, may reduce or even satisfy the level of effort needed to comply with the HIPAA Security Rule.
- Define goals and objectives of the crosswalk
  Example: The primary goal of the crosswalk is to better understand the compliance requirements of the HIPAA Security Rule.

C. Create a template for capturing the relevant security requirements

An Excel spreadsheet is an acceptable, easy tool in which to construct a matrix, for documenting the specific areas from the HIPAA Security Rule and the selected security standard for the crosswalk in this example.

Sample CROSSWALK TEMPLATE -The crosswalk table below provides a format for the development of a matrix for a comparison of the requirements, and the subsequent analysis to determine where actions to ensure compliance are necessary. Disclaimer: The contents of this sample chart are for illustrative purposes only, and not to be interpreted or accepted as real crosswalk data. The author of the paper did not perform the below crosswalk analysis, it is hypothetical information.

REFERENCE NUMBER	HIPAA REQUIREMENT	SOURCE	ADD SUBJECT OF CROSSWALK
	Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.	HIPAA Security Rule 164.308(a)(1)(i)	
	Risk Analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	HIPAA Security Rule 164.308(a)(1)(ii)(A)	
	Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with HIPAA Security Rule Section 164.306(a).	HIPAA Security Rule 164.308(a)(1)(ii)(B)	
	Sanction Policy (R): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	HIPAA Security Rule 164.308(a)(1)(ii)(C)	

REFERENCE NUMBER	HIPAA REQUIREMENT	SOURCE	ADD SUBJECT OF CROSSWALK
	Information System Activity Review (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	HIPAA Security Rule 164.308(a)(1)(ii)(D)	

There are other relational databases that can be deployed to create the mapping matrix. If the detailed analysis of the crosswalk is to be shared widely within an organization, it is important that a user-friendly and easily accessible template be selected.

For illustrative purposes of a more technical approach template, see the sample SRTM template below. [10]

Sample SECURITY REQUIREMENTS TRACEABILITY MATRIX (SRTM)

This table contains the security requirements traceability matrix between the set of security requirements and the security test activity. The security requirements traceability matrix below provides a format for the development of a matrix for a security test activity.

REQUIREMENT IDENTIFICATION NUMBER	REQUIREMENT DESCRIPTION	REQUIREMENT SOURCE	TEST OBJECTIVE(S)	VERIFICATION METHOD(S)
This column contains a unique identifier for each requirement (e.g., 100)	This column contains a description of each requirement to be verified in the security test activity.	This column cites the source of the requirement.	This column lists the individual test objectives which are used to show compliance to the stated requirement. A stated requirement may have one or more test objectives associated with it.	This column lists the verification method used to verify the test objective.
Legend: Verification Methods A = Analysis D = Demonstration I = Inspection T = Test				

D. Determine the level of granularity for data capture

For thoroughness and completeness, it is recommended that actual excerpts of the language from the two standards to be “crosswalked” are cut and pasted or typed into the template. Alternatively, only the first line

or paragraph of a specific standard can be excerpted. The level of detail is a subjective decision. But the more complete the language about a specific security requirement that is actually captured in the template, the better. The additional detail helps to make the interpretation and analysis as to the degree of compliance with a security requirement easier in the later steps.

E. Populate the template with comparative security requirements language from the selected standards

Proceed to copy and paste the first sentence, paragraph, key words or a summary statement from the security requirements being compared. It is important to be consistent. The level of detail must be able to be enough so that an analysis or judgment can be made about the degree of potential coverage. The important point is to include the sources for the language lifted so that conclusions can be well documented. Disclaimer: The contents of this sample chart are for illustrative purposes only, and not to be interpreted or accepted as real crosswalk data. The author of the paper did not perform the below crosswalk analysis, it is hypothetical information.

HIPAA ADMINISTRATIVE SAFEGUARD - §164.308		
CRITERIA TO MEET SAFEGUARD	**APPLICABLE FISMA REQUIREMENT**	**INCLUDED IN DITSCAP (Phase 2: Verification and Phase 3: Validation)**
(a)(5). Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management).	**Ref §3544(b)(4)** ‘‘security awareness training to inform personnel, including contractors and other users of information systemsthat support the operations and assets of the agency, of—‘‘(A) information security risks associated with their activities; and‘‘(B) their responsibilities in complying with agencypolicies and procedures designed to reduce these risks;	**Ref 8510.1, DITSCAP Section 5.3.9.2.4.** "Verify that Security Rules of Behavior, a Security Awareness and Training Program, and an Incident Response Program are in place, are current and effective." **DITSCAP, Appendix O, Security Education, Training, and Awareness Plan. Mandated by DoDD 8500.1, § 4.22.** "All personnel authorized access to DoD information systems shall be adequately trained in accordance with DoD and component policies and certified as required in order to perform the tasks associated with their IA responsibilities."
(A). Security Reminders: Implement periodic security updates.		
(B). Protection from Malicious Code: Implement Procedures for guarding against, detecting, and reporting malicious software.		
(C). Log-in Monitoring: Procedures for monitoring log-in attempts and reporting discrepancies.		
(D). Password Management: Procedures for creating, changing, and safeguarding passwords.		

F. Conduct and analysis as to where there is some degree of coverage or potential satisfaction (compliance) for each requirement

This step is highly subjective. A summary sheet can be prepared to indicate at a high level using checkmarks, or numerical values or color-coding to indicate the degree to which a security requirement may be satisfied. At a minimum, there may be three ranges indicated:

High: (Green) – Great degree of similarity and overlap between the two security requirements or standards.
Medium: (Yellow) - Some potential overlap, with some degree of modification or change in the existing policy or procedures; there is something to leverage
Low: (Red) -No overlap, out of scope or non-complaint or non-applicable.

Below is a sample summary chart for a high-level presentation of the potential areas of overlap and other areas of potential exposure in a HIPAA Security Rule and DITSCAP crosswalk. Disclaimer: The contents of this sample chart are for illustrative purposes only, and not to be interpreted or accepted as real crosswalk data. The author of the paper did not perform the below crosswalk analysis, it is hypothetical information.

HIPAA SAFEGUARD	CRITERIA TO MEET SAFEGUARD	INCLUDED IN DITSCAP	RISK
Technical	**Access Controls**	Yes	**LOW**
	Unique User Identification	Yes	**MEDIUM**
	Emergency Access Procedure	Yes	**MEDIUM**
	Automatic Logoff	Yes	**MEDIUM**
	Encryption and Decryption	No	**HIGH**
	Audit Controls	Yes	**LOW**
	Person or Entity Authentication	Yes	**LOW**
	Integrity	Yes	**LOW**
	Mechanism to authenticate Electronic Protected Health Information	No	**HIGH**
	Transmission Security	Yes	
	Integrity Controls	No	**HIGH**
	Encryption	No	**HIGH**

G. Summarize the results and create an action plan

It is recommended that those security requirements where there is a red color-coding, or an indication of low degree of satisfaction be ranked for immediate or first attention in the action plan. An action plan should document the decisions made as to how to close and gaps, or clearly non-

compliant subject areas. An action plan could include the major milestones, with realistic dates for completion of the corrective measures, and an estimate of resources required to resolve the issue so that management can monitor the completion.

V. Rationale for Crosswalking Security Requirements

In the absence of one definitive security regulatory regime, many sectors establish their own security standards (though often slowly and while under considerable pressure and threat of government action) in an effort to bring order, consistency, and efficiency to their business environment and to address current and real problems in the marketplace. For example, on February 7, 2003 the Direct Marketing Association (DMA) issued a press release announcing new guidelines for "protecting personal information from data thieves and released a new security checklist developed with the Federal Trade Commission (FTC)." The purpose of these security guidelines is to combat the growing problem of identity theft. 11]

Another example of this movement by the private sector to fill the void where no one security standard exists is the formation of the Cyber Security Industry Alliance, a security trade group founded in February 2004 by eleven companies, "to influence public policy and spending on cyber security."[12]

The year one goals as outlined on the Cyber Security Industry Alliance Web Site include activities in four main areas:

- "Public policy**…**
- Education…
- Awareness…and
- Standards: in partnership with other organizations, we will identify and support emerging industry technology standards."[13]

With regards to the security standards, the Cyber Security Industry Alliance advocacy group recognizes that there is no comparable "generally accepted information security principles" as exists for the financial services or accounting industry. This group, whose membership is comprised of mostly computer security firms, hope "to push to have the federal government adopt generally accepted information security principles."

Consider for a moment the role of the Financial Accounting Standards Board (FASB) within the financial sector. The stated mission of the FASB is "to establish and improve standards of financial accounting and reporting for the guidance and education of the public, including issuers, auditors and users of financial information." [14] The FASB has a trusted relationship with the U.S. Security and Exchange Commission (SEC), whose primary mission "is to protect investors and maintain the integrity of the securities markets." [15]

The SEC accepts the FASB self-regulatory process of establishing the necessary accounting standards and practices that are voluntarily implemented within corporate America. How much easier would the world of information security be if there was a similar symbiotic relationship with one accepted security standards making body and one oversight institution instead of the plethora of security standards that exist for the private sector today?

The Cyber Security Industry Alliance sees benefits to having a common set of information security principles. They have also expressed support for the Federal government's "information technology product and systems certification program known as the National Information Assurance Partnership (NIAP)." The stated long-term goal of the NIAP partnership is "to help increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and validation programs. In meeting this goal, NIAP also lists setting standards as one of its priorities as it seeks to: "Promote the development and use of evaluated IT products and systems;

- Champion the development and use of national and international standards for IT security;
- Foster research and development in IT security requirements definition, test methods, tools, techniques, and assurance metrics;
- Support a framework for international recognition and acceptance of IT security testing and evaluation results; and
- Facilitate the development and growth of a commercial security testing industry within the U.S." [16]

In their kick-off press release, the Cyber Security Industry Alliance highlight the fact that the Chairman of the House Government Reform Committee's Technology, Information Policy, Intergovernmental Relations and the Census Subcommittee, Representative Adam Putnam (R-Florida) issued a statement supporting the new alliance. In a statement issued on February 25, Rep. Putnam praised the group for its focus on cyber security, which he called a critical issue "with potentially far-reaching ramifications to the American people and the U.S. economy." Rep. Putnam, as the youngest current member of the U.S. House of Representatives, is recognized for being a champion on computer security related matters. [17]

On a separate issue, Putnam made the news recently by suggesting that he may propose legislation "that would make security requirements regarding protecting computer networks, similar to those presently imposed on U.S. Federal agencies, mandatory for privately held companies too." [18] Requiring annual risk assessments for all publicly held companies would be a new uniform security standard for the private sector that Federal agencies are already implementing in accordance with the E-Government Act of 2002. [19]

In the transcript of a live chat on technology issues for on Washington Post's Web Site on February 12, 2004, Putnam responded to a question about the proposed security regulations for privately held companies by indicating that he had made a decision to delay introducing legislation that would mandate cyber security standards for the private sector because he "came to the conclusion that I had raised the point and the awareness sufficiently in the boardrooms so that the private sector would take IT Security seriously. If they can come up with a plan that establishes sound practices, adhered to by the industry, I would support such a meaningful security plan even if it did not require direct Federal law. There were also concerns about writing technology standards into the law that would be obsolete soon, and great concerns over the SEC role in technology -- one they are not equipped to handle." [20]

Yet another study group of private and public sector security experts are reportedly now studying this issue. How successful the private sector will be in developing these needed security standards for themselves is yet to be seen. Due to the increase in security related regulations, such as HIPAA, Gramm-Leach-Bliley, Sarbanes Oxley, and the others listed at the onset of this paper, C-level executives are having to pay attention to IT security policies that were previously delegated within the organization, since failure to comply may result in penalties including fines and even their own imprisonment. It is probable that the issue of security standards may resurface on the U.S. Congressional agenda again in the near-term if the self-defining and self-policing approach does not produce the desired successful results.

The fact that there are many optional sets to security standards, but no one definitive source for security standards and industry best practices for private companies, makes the corporate CIO's job uniquely challenging. Conversely, the U.S. government Federal agency CIO has its list of security mandates, with specific oversight from the Government Accounting Office (GAO), the Inspector General (IG) and other numerous periodic performance monitoring and evaluation sources.

The U.S. Chief Information Officers' Council, (the CIO Council) is a group established in the Clinger-Cohen Act and codified by the E-Government Act of 2002, whose membership includes the Chief Information Officers from the major U.S. Federal government agencies. The CIO Council, as noted on their Web Site, is the "principal interagency forum to improve agency practices for the management of information technology." The CIO Council includes improving security standards as one of its central objectives:

- "Work as appropriate with the National Institute of Standards and Technology and the Administrator of the Office of Electronic Government and Information Technology (OMB) to develop recommendations on information technology standards developed under section 20 of the

National Institute of Standards and Technology Act (15 U.S.C. 278g-3) and promulgated under Section 11331 of Title 40, and maximize the use of commercial standards as appropriate, including the following:

- Standards and guidelines for interconnectivity and interoperability as described under section 3504
- Consistent with the process under section 207(d) of the E-Government Act of 2002, standards and guidelines for categorizing Federal government electronic information to enable efficient use of technologies, such as through the use of extensible markup language
- Standards and guidelines for Federal government computer system efficiency and security "[21

Even with these prescribed security standards, the Federal agencies' CIOs' job can still be as problematic as that of private company CIOs. The difficulty for both private and public sector CIOs arises as they attempt to implement, monitor, and report efficiently about all of the many, often interdependent, overlapping and duplicative, mandatory and known best practices security requirements. This is where a security requirements crosswalk exercise would be useful to both.

VI. Crosswalking Conclusions

A. Benefits of Crosswalking Security Requirements

The crosswalk exercise results can be used by the CIO to help build a business case for more investment in needed security related resources in order to comply with requirements. The cost of compliance verses the potential financial losses associated with a violation, depending upon the infringement, the enforcement mechanisms and consequences that can include fines, negative publicity, and other immeasurable consequences, are easily outlined though not often specifically calculated. For example, there is no value that can be placed on the loss of a life that may result from corrupted data due to a computer virus going into a medical device and the wrong medication being administered to a patient. When these real world, and unfortunately true instances of problems that can occur due to poor security management are revealed, the benefits of a security crosswalk and subsequent implementation of an action plan become apparent.

The crosswalk analysis can reveal to the CIO and other senior executives where there are already polices, procedures, processes, and tools in place to meet and comply with the HIPAA Security Rule by virtue of existing security operations. In addition, the crosswalk can highlight where adjustments in the current state can be made with minimal effort to ensure compliance. The summary analysis can indicate where there is a potential problem or an issue area that is not addressed to the required degree and immediate action may be necessary to endure compliance with HIPAA. Finally, this crosswalk methodology can possibly serve

as a bridge among the various stakeholders described above whom may have conflicting objectives.

Security and healthcare professionals need not feel alone in their efforts to comply with the security related legislation and to implement appropriate security standards. In addition to Federal government resources, there are several supplemental sources that an organization can turn to for help and/or additional information, including industry associations as well as academic orientated security resources. A few examples are highlighted herein, but their mention and inclusion in no manner implies an endorsement of their products, services or offerings. (Note: All of the URLs for the sources below are listed in the References Section of this paper). [22]

B. Associations

There are many other groups that are seeking ways to help their membership implement security best practices.

For example:

- There is a Security Health Care Certification and Accreditation Workgroup co-facilitated by URAC/NIST/WEDI whose mission is "to bring together stakeholders from the public and private sectors to facilitate communication and consensus on best practices for information security in healthcare and to promote the implementation of a uniform approach to security practices and assessments by developing white papers and crosswalks, and provide education programs, as appropriate."

- The Health Information Management Systems Society (HIMSS) – "is the healthcare industry's membership organization exclusively focused on providing leadership for the optimal use of healthcare information technology and management systems for the betterment of human health. HIMSS frames and leads healthcare public policy and industry practices through its advocacy, educational and professional development initiatives designed to promote information and management systems' contributions to ensuring quality patient care." It also has a HIPAA Shared Interest Group (SIG) who have a "member only listserve" and frequently discuss issues such as are the HIPAA Final Security rule implementation.

- The Internet Security Alliance – "is a non-profit collaboration between EIA and Carnegie Mellon's CERT Coordination Center (CERT/CC), with a diverse and international membership." They have published and make available on their Web Site complimentary "Common Sense Security "guides for senior managers and home and individual use.

C. Academic Orientated Security Resources

There are a wealth of white papers and commentaries available, complimentary via the web, recommended start points:

- The HIPAA Advisory
- The SANS Reading Room

Some of these documents address the more technical aspects of security compliance and controls verses the security related legislation and standards, which was the focus of this paper.

D. Commercial Vendors and Consultants

Lastly, there are also numerous commercial vendors and consultants who offer products, software and services to help organizations complete security risk assessments, a security requirements traceability matrix (SRTM), and other security related documentation and compliance activities.

A security crosswalk is but one approach an organization can take to answer the question proposed at the onset of this paper: "where to begin on the road towards security compliance?" Whether dealing with a large global corporate enterprise; a Federal agency implementing an e-government initiative; or a small rural family home-based business; determines what security regulations are mandatory. Where one starts, dictates the best path. The goal of the crosswalk exercise is to build upon existing security practices that may be in place as one proceeds down the path to security compliance. There are other self-assessments, gap-analysis, risk assessment tools, and security audits that can be pursued to assist in the goal to achieve compliance with HIPAA as in the example explored herein, or other security standards.

VII. References

[1] Links to the selected security related legislation mentioned and/or quoted are provided:

SELECTED LEGISLATION	URLS
Government Performance and Results Act (GPRA)	http://www.whitehouse.gov/omb/mgmt-gpra/
Government Paperwork Elimination Act (GPEA)	http://www.whitehouse.gov/omb/fedreg/gpea2.html
Government Information Security Reform Act (GISRA replaced by FISMA)	http://www.whitehouse.gov/omb/memoranda/m01-08.pdf
Gramm-Leach-Bliley Act	http://banking.senate.gov/conf/
Sarbanes-Oxley Act	http://banking.senate.gov/pss/acctrfm/conf_rpt.pdf
Clinger-Cohen Act	http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
Health Insurance Portability and Accountability Act (HIPAA)	http://www.cms.hhs.gov/hipaa/
E-Government Act of 2002	http://www.cio.gov/documents/e_gov_act_2002.pdf
Federal Information Security Management Act of 2002 (FISMA)	http://www.fedcirc.gov/library/legislation/FISMA.html

[2] Links to the selected security standards mentioned and/or quoted are provided:

SELECTED SECURITY STANDARDS	URLS
National Institute of Standards and Technology (NIST) 800 Series Publications	http://csrc.nist.gov/publications/
Department of Defense Information technology Security Certification and Accreditation Process (DITSCAP)	http://www.tricare.osd.mil/tmis_new/Policy/DoD/i520040p.pdf
Various DoD Directives	See DOD Section, Policy and Guidance http://www.tricare.osd.mil/tmis_new/Policy/DoD/p52001r.pdf
OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation℠)	http://www.cert.org/octave/
American National Standards Institute (ANSI)	http://www.ansi.org/
International Organization for Standardization (ISO) 17799	http://www.iso17799software.com/
International Electrotechnical Commission (IEC)	http://www.iec.ch/
System Security Engineering Capability and Maturity Model (SSE CMM)	http://www.sse-cmm.org/

[3] Hippocratic Oath—Classical Version. Translation from the Greek by Ludwig Edelstein. Baltimore: John Hopkins Press, 1943.
URL: http://www.pbs.org/wgbh/nova/doctors/oath_classical.html

[4] The Hippocratic Oath Today: Meaningless Relic or Invaluable Moral Guide? , NOVA Online, Survivor M.D.
URL: http://www.pbs.org/wgbh/nova/doctors/oath_today.html

[5] American Medical Association Web Site, E-History
URL: http://www.ama-assn.org/ama/pub/category/8291.html

[6] Centers for Medicare and Medicaid Services (CMS) Web Site, HIPAA Administrative Simplification - Overview
URL: http://www.cms.hhs.gov/hipaa/

[7] Centers for Medicare and Medicaid Services (CMS) Web Site, HIPAA Administrative Simplification – Security, Final Rule
URL:http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp

[8] Links to the selected healthcare related standards mentioned and/or quoted are provided:

SELECTED HEALTHCARE SECTOR STANDARDS/ACCREDITATIONS	URLS
The Joint Commission on Accreditation of Healthcare Organizations (JCAHO)	http://www.jcaho.org/
CMS Core Security Requirements (CMS CSR)	http://www.cms.hhs.gov/manuals/pm_trans/AB03005.pdf
CMS Internet Security Policy	http://www.cms.hhs.gov/it/security/docs/internet_policy.pdf
URAC Security Audit Service	http://www.itsecurity.com/tecsnews/jan2004/jan185.htm
NCQA Certification and Accreditation Standards	http://www.ncqa.org/index.asp

[9] Definition of SRTM excerpted from DoDIIS Security Certification & Accreditation Guide, April 2000, URL:http://www.rl.af.mil/tech/programs/jitf/tpoc/downloads/nov00/security_cert.pdf.

[10] Sample SRTM excerpted from MHS/Tricare Web Site, System Security Test Preparation Guide, 31 January 1996, Prepared for Defense Information Systems Agency (DISA), Version 1.0
URL: http://www.tricare.osd.mil/

[11] Hovanyetz, Scott, "DMA, FTC Release Data Security Guidelines,: DMNews, February 7, 2003
URL: http://www.dmnews.com/cgi-bin/artsearch.cgi?keywords1=%22FTC+Release+Data+Security+Guidelines%22&words=all&category=0&from_month=&from_day=&from_year=&to_month=&to_day=&to_year=&search=search

[12] Olsen, Florence, "Security Trade Group Formed," Federal Computer Week, February 26, 2004, URL: http://www.fcw.com/fcw/articles/2004/0223/web-security-02-26-04.asp

[13] Cyber Security Industry Alliance Web Site, "Goals for Our First Year,"
URL: http://csialliance.org/aboutus/goals.html

[14] Financial Accounting Standards Board (FASB), 'A Mission for Neutral Standards
URL: http://www.fasb.org/facts/index.shtml

[15] U.S. Securities and Exchange Commission Web Site, "The Investor's Advocate: How the SEC Protects Investors and Maintains Market Integrity"
URL: http://www.sec.gov/about/whatwedo.shtml

[16] National Information Assurance Partnership (NIAP) Web Site, "Goals of the Partnership."
URL: http://niap.nist.gov/

[17] Congressman Adam H. Putnam Web Site,
URL: http://www.house.gov/putnam/

[18] Chabrow, Eric, "Congressman May Introduce Bill to Mandate Risk Assessments, Information Week, November 3, 2003
URL:
http://www.informationweek.com/story/showArticle.jhtml?articleID=15800647

[19] E-Government Act of 2002,
URL:http://www.cio.gov/documents/e_gov_act_2002.pdf.

[20] Krebs, Brian, "Congress and Cyber Security," washingtonpost.com, February 12, 2004
URL: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A26684-2004Feb9&notFound=true

[21] Chief Information Officers Council (CIO) Web Site, Chief Information Officers Council Charter, December 15, 2003
URL:
http://www.cio.gov/index.cfm?function=councildescription&subsection=councilcharter

[22] Links to the selected alternative sources of information mentioned and/or quoted are provided:

SUPPLEMENTAL INFORMATION SOURCES	URLS
Security Health Care Certification and Accreditation Workgroup co-facilitated by URAC/NIST/WEDI	http://webapps.urac.org/committesite
Health Information Management Systems Society, (HIMSS), Shared Interest Group (SIG)	http://www.himss.org/ASP/index.asp
Internet Security Alliance	http://www.isalliance.org/
HIPAA Advisory	http://www.hipaadvisory.com/action/security/
SANS Institute Reading Room	http://www.sans.org/rr/