USING NIST FOR SECURITY AND RISK ASSESSMENT

Tom Dover
Butler County Community College

Butler County Community College

Using NIST for Security and Risk Assessment

Tom Dover

The LibreTexts libraries are Powered by NICE CXOne and are supported by the Department of Education Open Textbook Pilot Project, the UC Davis Office of the Provost, the UC Davis Library, the California State University Affordable Learning Solutions Program, and Merlot. This material is based upon work supported by the National Science Foundation under Grant No. 1246120, 1525057, and 1413739.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation nor the US Department of Education.

TABLE OF CONTENTS

Book Information

TITLE

Using NIST for Security and Risk Assessment

SHORT TITLE

Using NIST Special Publications (SP) 171r2/172 and 213/213A for Security & Risk Assessment

SUBTITLE

Protecting Controlled Unclassified Information (CUI) in Information and Operation Technology Systems

SHORT DESCRIPTION

A practical approach for applying NIST Special Publications (SP) guidance to Information (IT) and Operational (OT) technology systems. Methodology includes assessing and evaluating the security of systems containing Confidential but Unclassified Information (CUI).

AUTHOR(S)

Thomas P. Dover
thomas.dover@bc3.edu

PUBLICATION DATE

07/10/2022

COPYRIGHT

(2nd Edition)

OER LICENSE

BOOK TAGLINE

Applying NIST Guidance to Cybersecurity Assessment

PRIMARY SUBJECT

Computer Security

ADDITIONAL SUBJECTS

Risk Assessment, Information Technology Industries, Network Security, Computer Science

LONG DESCRIPTION (Abstract)

This book describes how NIST Special Publications (SP) 800-171r2 (*Protecting Controlled but Unclassified Information in Nonfederal Systems and Organizations*), SP.800-172 (*Enhanced Security Requirements for Protecting Controlled Unclassified Information*) and SP.800-172A (*Assessing Enhanced Security Requirements for Controlled Unclassified Information*) can be used to evaluate the cybersecurity posture of Information (IT) or Operation Technology (OT) systems and supporting frameworks. It will demonstrate that baseline security requirements outlined in SP.800-171r2 and SP.800-172/172A for the protection of Controlled Unclassified Information (CUI) can be applied to any information system requiring data protection.

It further presents the application of SP.800-213 (*IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*) and SP.800-213A (*IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirement Catalog*) to OT system assessment in order to determine relative compliance with recommended standards. This approach allows organizations to evaluate the level of risk an IoT device poses to information systems. It also reviews the current state of IoT cybersecurity and privacy protection using historical and current industry guidance & best-practices; recommendations by federal agencies; NIST publications; Executive Orders (EO) and federal law. Similarities and differences between IoT devices and “traditional” (or classic) Information Technology (IT) hardware will be offered along with challenges IoT poses to cybersecurity and privacy protection.

An explanation of how these NIST publications align with information security and how this alignment suffices for evaluating an IT environment security will be given along with the process and procedure for performing such evaluation.

Licensing

*A detailed breakdown of this resource's licensing can be found in **Back Matter/Detailed Licensing**.*

Author's Note

The approach offered here for security and/or risk assessment is presented from the perspective of the healthcare sector. In other words, the laws and regulations which govern the healthcare industry--HIPAA and HITECH--serve as security requirements for assessment and evaluation. It should be stressed, however, that the approach is designed as industry-neutral and can be applied to any business sector (e.g., finance, manufacturing, education, etc..).

Preface

This book was born out of necessity.

As an Information Security Specialist in the healthcare sector I needed a framework for evaluating Security and Risk in my IT environment that was also granular enough for me to determine compliancy with industry best-practices or standards. As my environment was becoming increasingly complex and diversified I realized a single-focus security/risk assessment was insufficient. I needed a method for both quantitatively and qualitatively assessing the security posture of my environment.

But where to start? While aware of the requirements for information security imposed by federal law—the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH)—I was unable to find a publicly available tool or published approach sufficient enough to evaluate compliance and simple enough to use without special software or training.

While various security and/or risk assessment frameworks exist such as the International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) few include methodology for gauging compliance. Most formal security/risk assessments are commercial offerings, however, the Department of Health and Human Service, Security Risk Assessment (SRA) is freely available.

As I have been using NIST security publications for some time I decided it may be a good place to start. The single drawback to using NIST as a standard, however, is that its guidance is chiefly directed at federal agencies and not the private sector. As NIST has taken on an expanded role in Cybersecurity research and publication, however, it has emphasized its publications as applying to non-government organizations (NGO) as well. I have also found that while commercially available SRAs may incorporate NIST standards they usually lack insight into which publications—or portion(s) thereof—are used in their products. This makes determining compliance challenging since a baseline for comparison is not possible.

After researching the issue I came to the conclusion that I would have to develop a new approach for achieving my security assessment need. Fortunately, I was able to create this approach using NIST Special Publication (SP) series; specifically those for protecting “Controlled but Unclassified Information” or CUI. I was further able to use publications specific to data security for Operational Technology (i.e., Internet of Things or IoT). In effect, through NIST publications I was able to develop security assessments for both Information and Operational Technology using a common quantitative and qualitative framework.

Security/Risk Assessment is a fundamental task necessary for the protection of the Confidentiality, Integrity and Availability (CIA) of information. Unlike other NIST publications used for Cybersecurity, the security requirements used in this book for Information Technology are unique in that they specifically omit security requirements exclusive to the federal government. In other words, NIST’s guidance for protecting Controlled Unclassified Information (CUI) can be applied, in totality, to non-government organizations (NGO) without first having to be distilled of those security requirements exclusive to federal IT systems. Although its publications provide essential frameworks and methodology for security/risk assessment NIST guidance lacks the steps necessary for determining *compliance.* Generally speaking, NIST publications tell you *what* has to be protected and to what extent) to achieve a certain level of security (i.e., Low, Medium or High)) but does not provide instructions on how-to accomplish this goal. This omission, however, is partly by design. NIST publications tend to be written with flexibility and adaptability in mind. These attributes are important when applied to organizations of different sectors and sizes.

This book enhances NIST publication guidance by augmenting the assessment process. Augmentation includes:

- Security Requirement ‘Satisfying’ statement
- Validation Point Tool
- Security Control Type (Healthcare only)
- Assessment Evaluation
- Statistical Analysis Summary

These features serve to enhance Security/Risk Assessment by including not only core NIST elements for identifying weaknesses & vulnerabilities, and identifying risk but determining the level of compliance (via simple statistics) of an organization’s IT environment. This knowledge can be used to satisfy regulatory or legal compliance, gauge organizational change, and assess compliance relative to established industry standards and recommendations.

I hope you find it useful.

Thomas P. Dover
thomas.dover@bc3.edu

Scope

The process and procedures presented in this book are directed at the protection of information, indirectly or directly, that is designated by an organization to be Controlled but Unclassified Information (CUI). The word "Unclassified" is used within the context of federal government Information Systems. For the purpose of this discussion, however, 'Unclassified' information is any data deemed sensitive, company-confidential, or whose public disclosure would harm or interfere with normal business/organizational operations.

For example, in healthcare, patient information (per HIPAA) is considered *electronic Protected Health Information* (ePHI) which requires protection from unauthorized access or disclosure. In this context patient information is considered CUI since the principles for information security and protection apply.

While CUI does not directly apply to Operational Security (i.e., Internet of Things) the principles of information security and protection apply but are supplemented by additional security requirements involving data storage and transmission. It is further limited to Cybersecurity and privacy protection assessment & evaluation of IoT devices used by or for the healthcare sector as it relates to HIPAA[1] and HITECH[2] requirements for protection of electronic Protected Health Information (ePHI). It should be noted, however, that the security requirements outlined for Medical IoT devices (MIoT) are applicable to any IoT device.

This book does not address action(s) necessary for correction or mitigation (i.e., Reduce, Avoid, Accept, Transfer).

---

1. Health Insurance Portability and Accountability Act (HIPAA). 1996.

2. Health Information Technology for Economic and Clinical Health (HITECH). 2009.

Target Audience

This book is intended for both student and practitioner.

Students will find it useful for learning about the National Institute of Standards and Technology (NIST) approach to Information & Operational Security (IT/OT) and Cybersecurity and how to use NIST publications for practical security assessment.

Practitioners tasked with conducting security assessments of Information or Operational Technology Systems will benefit from NIST best-practices and guidance which can be applied to real-world challenges as well as incorporated into an organization's Risk Management Program.

Finally, those responsible for the administration, management or oversight of Information systems which create, handle, store or transmit Controlled but Unclassified Information (CUI) or Internet of Things (IoT) devices responsible for collecting and transmitting such information will find it helpful for determining how well their security practices comply with industry-standards or Best Practices.

Prerequisites

Due to technical aspects of the material the recommended (but not required) background for completing a security/risk assessment includes working knowledge of:

- network technology
- desktop and mobile technology
- access control & identity management
- protection of controlled information

Acknowledgements

Book cover image (clipboard) courtesy of Glenn Carstens-Peters at unsplash.com

Keywords

Security Assessment, Security Analysis, Security Evaluation, Security Review, Risk Analysis, Risk Assessment, Electronic Protected Health Information, ePHI, HIPAA, Privacy Rule, Security Rule, HITECH, Healthcare sector, HHS, NIST, FDA, Controlled Unclassified Information, CUI, Internet of Things (IoT), Medical Internet of Things (MIoT), SP.800-171r2, SP.800-172, SP.800-213, SP.800-213A.

CHAPTER OVERVIEW

1: Introduction

1.1: The Distributed Challenge of Security and Risk Assessment

In some ways, conducting a security or risk assessment has shifted from a relatively straightforward task to a complex undertaking. Hosted and Cloud-based computing stand out as having contributed to this increased complexity due to their design and architecture.

For example, it used to be that an application was (or could be) developed, hosted and maintained by a single company or organization. Since hardware and software resources would be under a company's direct control, oversight and access to information needed for a security or risk assessment was readily available and easily mapped to security requirements. With the advent of distributed/Cloud computing, however, information about an application's operation, performance and security are split among one or more organizations. The responsibility for security then becomes "shared" and identifying who is responsible for what (and when) may result in "gaps" in needed information. Moreover, since no two companies or organizations are alike (or operate alike) their approach to information and system security may be quite different. The challenge, therefore, in a distributed technology environment becomes how to best apply a common set of security standards or requirements uniformly among individual company or organizations in order to produce an accurate and balanced assessment.

In healthcare the federal government addresses the issue of shared-responsibility in Part 1, Section 13401 of the HITECH Act. It applies HIPAA's Administrative, Physical and Technical Safeguards provisions to any *Business Associate* who handles Electronic Protected Health Information (ePHI). Moreover, it makes Business Associates responsible for the protection of sensitive information "in the same manner that such sections apply to the *Covered Entity*"[1]. Since each company or organization (Covered Entity or Business Associate) are required to meet the same level of security, assessment becomes simpler since security requirements are applied equally regardless of business designation.

Similar provisions in other industry regulations (PCI, SOX) apply to other sectors such as Finance, Manufacturing and Energy.

Regardless of industry or sector the responsibility to protect sensitive information (e.g., financial, academic, healthcare) is born equally by any company or organization which has access to or otherwise "touches" (create, store, manipulate, transmit) sensitive or controlled data.

In shared-security systems the requirements for Security/Risk Assessment do not change but the ability to (accurately) evaluate such system may. It becomes essential then that the processes and methods used for assessing security in this type of environment be based on established guidelines or recognized industry-standards.

[1] Under HIPAA and HITECH, a *Covered En*tity (e.g., Hospital, Medical Practice) is the primary custodian of PHI and a *Business Associate* a contractor, sub-contractor or 3rd-party service provider.

1.2: Why use NIST?

Five reasons for using NIST publications:

1. NIST publications are processes & practices for federal government agencies to follow regarding Cybersecurity. Organizations partnering with the federal government are obligated to adopt these standards. Moreover, many organizations (public and private) adopt and adapt NIST standards for their own Cybersecurity and Risk Management programs.
2. NIST is often cited in federal laws, regulations, orders and statutes[1] as a source for Cybersecurity guidance. It is also cited by federal Departments[2] and agencies when promulgating rules and regulations governing specific critical sectors (e.g., manufacturing, health, finance).
3. NIST publications are used by private businesses and commercial vendors for the development of custom Cybersecurity and risk assessment programs. Some professional certifications in Cybersecurity are based on NIST standards.
4. NIST publications serve as an authoritative source for industry Cybersecurity “Best Practices”.
5. NIST publications are often cited in regulatory or legal proceedings as the basis for a company or organization’s Cybersecurity strategy or Risk Management Program.

[1] Examples include *IoT Cybersecurity Improvement Act of 2020*, passed in December, 2020; *HIPAA Safe Harbor Act*, an amendment to the *Health Information Technology for Economic and Clinical Health Act* (HITECH), signed into law in January, 2021; and Executive Order 14028 (*Improving the Nation’s Cybersecurity*), signed May 12, 2021.

[2] An example is the Department of Health and Human Services (HIPAA). See https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es for an example of NIST citation.

1.3: Regulatory and Legal Issues

Commonly held policies, procedures & practices for Cybersecurity can be traced to federal law or industry regulations. For example, the safety and security of medical information is linked to HIPAA[1], financial transactions to SOX[2] and credit card transactions to PCI DSS[3]. In each instance, compliance with specific requirements for information security and privacy are provided.

Moreover, many insurance companies require companies to adopt safeguards and technologies specifically designed to protection data and systems.

[1] Health Insurance Portability and Accountability Act

[2] Sarbanes-Oxley Act

[3] Payment Card Industry - Data Security Standard

1.4: FISMA

For NIST publications the *Federal Information Security Management Act* (FISMA) is a good way to demonstrate the link between laws and NIST publications. Originally passed by Congress in December, 2002. FISMA was updated in 2014 (Federal Information Security Modernization Act of 2014) but the essential elements of CIA for information security are retained in this update.[1] FISMA recognized the need for information security involving government information systems and directed federal agencies to develop programs for such protection. The law provided a framework for agencies to use that included the following areas:

- Inventory of Information Systems
- Categorize Information and Information Systems according to Risk Level
- Security Controls
- **Risk Assessment**
- System Security Plan
- Certification and Accreditation
- Continuous Monitoring

An important aspect of FISMA is its definition of information security:
"…protecting information and information systems for unauthorized access, use, disclosure, disruption, modification or destruction[2]…"

CIA
FISMA provides three elements that define information security and privacy:

CONFIDENTIALITY: "…preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information…"

INTEGRITY "...guarding against the improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity."

AVAILABILITY: "…ensuring timely and reliable access to and use of information."

Taken together the attributes of CIA comprise the basis of information security.

FISMA* (2002)

[1] FISMA was updated in 2014 (Federal Information Security Modernization Act of 2014) but the essential elements of CIA for information security are retained in this update.

[2] FISMA (Public Law 107-347), Section 3542. Definitions (b)(1)

1.5: FIPS 199 and 200

FIPS 199

FISMA* (2002)
→ FIPS 199 (2004)

Two years later (2004), NIST published **FIPS**[1] **PUB 199**, *Standards for Security Categorization of Federal Information and Information Systems*. This short (13 page) publication defined the potential impact on information and information systems in the event of a security breach (which it defined as the loss of CIA).

FIPS 199 categorized potential impact on "organizational operations, organizational assets or individuals" as **Low**, **Moderate** or **High** (Table 1).

Table 1 - Impact Level and Consequence

IMPACT	**CONSEQUENCE (to "organizational operations, organizational assets or individuals")**
Low	Limited
Moderate	Serious
High	Severe or Catastrophic

For security/risk assessment, 'consequence' is interpreted subjectively since consequence(s) can vary from one organization to another. For the purpose of discussion, however, a scenario involving a brick-and-mortar retail store might describe the consequence of an information system disruption as follows:

Limited: one or more sales registers have failed but backups and redundant systems keep transactions flowing with little noticeable disruption to either store operations or customer service.

Serious: one of more sales registers have failed and backup systems lag; unable to keep pace with transactions. Registers are shut down with noticeable disruption to store operations (i.e., long customer lines).

Severe or Catastrophic: one of more systems have failed and backup systems are non-existent or have also critically failed. Registers are unable to process transactions and business is halted. There is an obvious impact on store operations.

In each scenario, the ability to maintain *normal business operations* is adversely impacted and it is within this operational standard that the level of consequence (Limited, Serious, or Severe or Catastrophic) is defined.

FIPS 200

FISMA* (2002)
→ FIPS 199 (2004)
→ FIPS 200 (2006)

In 2006, NIST published **FIPS PUB 200**, *Minimum Security Requirements for Federal Information and Information Systems*. It specified minimum security requirements for (federal) information and information systems covering seventeen security-related areas[2]. As cited in FISMA, minimum security requirements are correlated to the level of adverse impact to Confidentiality, Integrity and Availability (CIA) caused by a data breach as outlined in FIPS 199. FIPS 200 also provided a methodology for determining an information system's security category (Low, Moderate or High).

Below is an example of FIPS 200 minimum security requirement as it pertains to **ACCESS CONTROL**:

Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

PUBLICATION LINKS

While some NIST publications serve as standalone guides others utilize associated publications which supplement or complement their particular topic. For example, the NIST Cybersecurity Framework[3] and Control Catalog (SP. 800-53r5)[4] reference one another. Likewise, when discussing security\risk assessment there is a connection between FISMA, FIPS and NIST SP.800 171r2/172[5].

FISMA* (2002)
→ FIPS 199 (2004)
→ FIPS 200 (2006)
→ SP.800-171r2/172 (2015)
*Note: FISMA is a law passed by Congress and not a NIST publication

[1] Federal Information Processing Standards (FIPS)

[2] This number has expanded and now consists of 20 areas (or *Security Control Families*) as outlined in NIST SP.800-53r5 (Security Control Catalog).

[3] Framework for Improving Critical Infrastructure Cybersecurity.

[4] Security and Privacy Controls for Information Systems and Organizations.

[5] SP.800-171 was originally published in June, 2015 with updates to it or its companion publications (800-172 & 800-172A) in 2016, 2019, 2020 and 2021.

1.6: Security Assessment Versus Risk Assessment- What's the Difference?

There are many sources available (both text and online) which can provide a detailed description of what Risk Assessment is and how to conduct one. While it is beyond the scope of this book to cover Risk Assessment understanding the difference between Security Assessment and Risk Assessment is important for information security. Therefore, a brief comparison of the two types is presented here.

Though their objective is the same (i.e., protecting information) Security Assessments differ from Risk Assessments in what is evaluated and how.

SECURITY ASSESSMENT

A *Security Assessment* or *Analysis* evaluates *requirements*, relative to a security control or control family[1] used to protect the Confidentiality, Integrity and Availability (CIA) of information. Once a solution for a security control is implemented the requirement is said to be *satisfied*.

For example, a control requirement may be:

Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)

Using role-based access might be one type of control which satisfies the requirement.

Security Assessments are often used to evaluate the overall security posture of an organization's information security program. Areas-of-concern can then be evaluated further for relative risk with appropriate steps taken to correct or mitigate identified problems. As with Risk Assessments, Security Assessments can be quantified in order to determine the strength of applied security as well as identifying weaknesses.

RISK ASSESSMENT

A *Risk Assessment* or *Analysis* identifies 1) **threats** to a system; 2) determines **vulnerabilities** (or weaknesses) a system possesses relative to the threat; and 3) evaluates the **likelihood** of the threat occurring and its **impact** on the system. Risk assessments are often, though not always, quantified in order to provide the *degree* or *level*[2] of risk. The basic formula for calculating risk is:

L(ikelihood[3]) x I(mpact) = R(isk)

Example Scenario: a small Datacenter [system] has no Uninterruptible Power Supply (UPS) [vulnerability or weakness] and is located in an area with a history of severe weather induced power outages [threat].

Given this information the *likelihood* of the threat (severe weather) occurring is evaluated as Low, Medium or High. The *impact* of the threat on a known vulnerability/weakness is then evaluated (Low, Medium or High). Using the L x I = R formula and substituting numeric values 1, 2 and 3 for Low, Medium and High labels a risk assessment might look like:

1. Threat = Severe Weather Power outage
2. Vulnerability/Weakness = No UPS
3. Likelihood (it is likely, given history, that severe weather will occur) = 3
   Impact (a power outage would disrupt Datacenter operations (no power) = 3
   Likelihood x Impact (3 x 3) = 9 (out of a possible 9).

Therefore, based on risk assessment the lack of UPS is a risk requiring mitigation.

Summarizing, Security Assessments evaluate overall system security whereas Risk Assessment determines risk based on Threat, Vulnerability (i.e., weakness) and Impact.

---

[1] NIST Control Catalog (SP.800-53r5) categorizes groups of security controls into *Families.* Examples of Control Families include Access Control and Configuration Management.

[2] Degree or level of risk depends on the risk assessment model used. Some models use simple Low, Medium and High labels with numeric values of 1, 2 and 3 whereas other models are more granulated (i.e., labels of Low, Low-Medium, Medium, Medium-High, High) with corresponding granulation for numeric values (1-5 or 1-10). There is no right solution and which numeric value(s) to use depends on the needs of the evaluator.

[3] The term 'probability' is sometimes used instead of *Likelihood* but both (essentially) have the same meaning.

CHAPTER OVERVIEW

2: Security Assessment Using SP.800-171r2 and SP.800-172

2.1: Introduction

In June, 2015 the National Institute of Standards and Technology (NIST) released Special Publication SP.800-171 (*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*). This publication was succeeded by SP.800-171r1 in December, 2016 and followed by SP.800-171r2 and its supplement SP.800-171B (*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Enhanced Security Requirements for Critical Programs and High Value Assets*) in June, 2019. The current version of SP.800-171r2 was released in February, 2020. SP.800-171B was renamed SP-800-172 (Draft) and released in July, 2020.

The purpose of SP.800-171r2 is to provide non-federal organizations[1] with guidance for protecting the Confidentiality[2] of unclassified (but controlled) information. As stated in its Abstract:

> *This publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category listed in the CUI Registry. The requirements apply to all components of nonfederal systems and organizations that process, store, or transmit CUI, or that provide security protection for such components.*

Though not specifically intended for Healthcare Delivery Organizations (HDO), security requirements contained in SP.800-171r2 are nevertheless applicable to the healthcare sector[3]. This is due, in part, to the Department of Health and Human Services (HHS) and Office of Civil Rights (OCR) references to NIST publications[4] in published documents and online guidance regarding cybersecurity protections and HIPAA's Security Rule. For example, HHS-OCR, Security Risk Assessment (SRA) Tool[5] references NIST publications in its User Guide. Moreover, vendors who develop security tools (e.g., IDS, antivirus, email protection) and Managed Security Service Providers (MSSP) often refer to NIST guidelines as "industry-standards".

In April, 2021, NIST released (Draft) SP.800-172A (*Assessing Enhanced Security Requirements for Controlled Unclassified Information*). Per NIST, "This generalized assessment procedures described in this publication provide a framework and starting point for developing specific procedures to assess the enhanced security requirements in NIST Special Publication 800-172[6]."

In effect, SP.800-172A uses *determination statements* and *Organization-defined parameters* as procedures for meeting assessment objectives. Meeting a determination statement results in a finding of *Satisfied* or *Other than Satisfied*. It then introduces three specific assessment methods (*Examine*, *Interview*, *Test*[7] for defining the "nature *and extent of the assessor's actions."* Also introduced are associated attributes *Depth* and *Coverage*.

Examine is "the process of checking, inspecting, reviewing…to facilitate understanding, achieve clarification or obtain evidence."

Interview is "the process of conducting discussions with individuals or groups…to facilitate understanding, achieve clarification or lead to the location of evidence."

Test is "the process of exercising one or more assessment objects under specific conditions to compare actual with expected behavior."

Each assessment method may contain one or more Object *Specifications*, *Mechanisms*, and *Activities*. These objects serve as evidence or proof through which assessment method requirements were met.

The attributes *Depth* and *Coverage* are used to describe the depth (i.e., rigor) and breadth (i.e., scope) of the assessment method review. For each method one of three values (*Basic*, *Focused* and *Comprehensive*) is used to describe the level of analysis.

Basic employs "high-level reviews, checks, observations or inspections of the assessment object."

Focused employs the above plus "more in-depth studies and analysis."

Comprehensive employs the above plus "detailed, and thorough studies and analyses of the assessment object."

As can be seen, each value represents a greater depth and breadth of analysis & review for a particular assessment method.

It should be noted that in its 'Cautionary Note'[8] statement NIST notes that the assessment methods and objects "do not necessarily reflect, and should not be directly associated with, compliance or noncompliance with the requirements."

An example of how to employ the assessment methods and their attributes of SP.800-172A are provided in Appendix A.

---

[1] Primarily federal contractors, or companies, agencies or organizations doing business with the federal government.

[2] Confidentiality is one part of the control triad for protecting sensitive information such as Electronic Health Record(s). The other parts of the triad are *Integrity* and *Availability*. Together, they form the CIA of cybersecurity.

[3] "…processing…healthcare data;" SP.800-171r2, p.1

[4] For example, the NIST Cybersecurity Framework and SP.800-53r5 (Control catalog) are often referenced in HHS regulations concerning protection of patient information.

[5] Available at The Office of the National Coordinator for Health Information Technology, Office of Civil Rights, Department of Health and Human Services (https://www.healthit.gov/topic/priva...ssessment-tool)

[6] See 'Cautionary Note', p. vi

[7] *SP.800-172A, Appendix C provides extensive description and explanation of all assessment methods and attributes.*

[8] Ch3, p.7

2.2: Process

The process for completing either SP.800-171r2 *(medium-level security requirement)* or SP.800-172/172A *(enhanced/high-level security requirement)* assessment consists of satisfying each control requirement then determining compliance for both individual and aggregate control families.

It should be stressed that SP.800-171r2 defines its control baseline security level as being for ***moderate-impact*** information systems and such level would cover healthcare-service providers handling, transmitting or storing electronic Protected Health Information (ePHI). SP.800-172 requirements are *enhancements* to SP.800-171r2 and therefore offer **stronger security** which would be needed for ***high-impact*** information systems. SP.800-172 contains thirty-four (34) enhanced security-control requirements and SP.800-172A offers assessment methods for evaluating assurance with SP.800-172 requirements.

An advantage of using both SP.800-171r2 and SP.800-172/172A is that security assessments can be performed from the perspective of both medium and enhanced-level security. Evaluating this way allows an organization to determine the level of compliance for each security level and to what extent it is being implemented.

In addition to control-requirement baseline, SP.800-172 has incorporated a new metric called Adversary Effects. Per NIST:

…adversary effects…describe the potential effects of implementing the enhanced security requirements on risk, specifically by reducing the likelihood of threat events, the ability of threat events to cause harm, and the extent of that harm. Five high-level, desired effects on the adversary can be identified: **redirect**, **preclude**, **impede**, **limit**, and **expose**."

For Adversary Effects, a simple (aggregate) matrix has been created to view the overall impact of security-control implementation.

An example of how to apply Adversary Effects is provided in Appendix B.

2.3: Methodology

Special Publication 800-171r2 utilizes FIPS-200[1] and SP.800-53r5[2] as the basis for its recommended Security Requirements. FIPS-200 defines the minimal security requirements for Low, Medium and High-impact information systems as outlined in FIPS-199[3]. NIST SP.800-53r5 identifies twenty (20) 'control families'. Control Families are security controls (applied to technology systems) which are operational, technical and management (i.e., administrative) safeguards used to protect the *confidentiality*, *integrity* and *availability* (CIA) of information systems and SP.800-171r2 utilizes a subset of these families. Control Families are groupings of security controls which address a specific security requirement. For example, *Access Control* deals with the methods, processes and/or procedures by which a user is granted access to a network or system.

SP.800-171r2 (and by association SP.800-172/172A) omits[4] seven control families contained in SP.800-53r5 that are specific to the federal government. It uses the remaining 13 'control families' but also incorporates a single, unique control family (*Security Assessment*). Together, these 14 control families form the basis for its one hundred ten (110) security-control requirements.

Table 1 displays SP.800-53r5 control families[5]. Those highlighted in gray/bold have been omitted from SP.800-171r2 security baseline requirements due to their unique 'federal' nature. Tailoring requirements in this manner makes application easier and results more accurate when applied to non-government sectors such as healthcare.

Access Control	Physical and Environmental Protection[6]
Assessment, Authorization and Monitoring	**PII Processing and Transparency**
Audit and Accountability	**Planning**
Awareness and Training	**Program Management**
Configuration Management	Risk Assessment
Contingency Planning	**System and Services Acquisition**
Identification and Authentication	*Security Assessment[7]
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity
Media protection	**Supply Chain Risk Management**
Personnel Security	

Table 1

[1] NIST Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems. Released March, 2006

[2] NIST SP.800-53r5, Security and Privacy Controls for Information Systems and Organizations. Released August 2017. Final draft published March, 2020

[3] NIST Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, NIST. Released February, 2004

[4]]"…some of the security requirements expressed in the NIST standards and guidelines are uniquely federal, the requirements in this publication have been tailored for nonfederal agencies." SP.800-171r2, p.3

[5] Note: Security Assessment is not an SP.800-53r5 control family. It is listed here for reference but is cited only in SP.800-171r2 and SP.800-172

[6] SP.800-171r2 cites this family as 'Physical Protection'

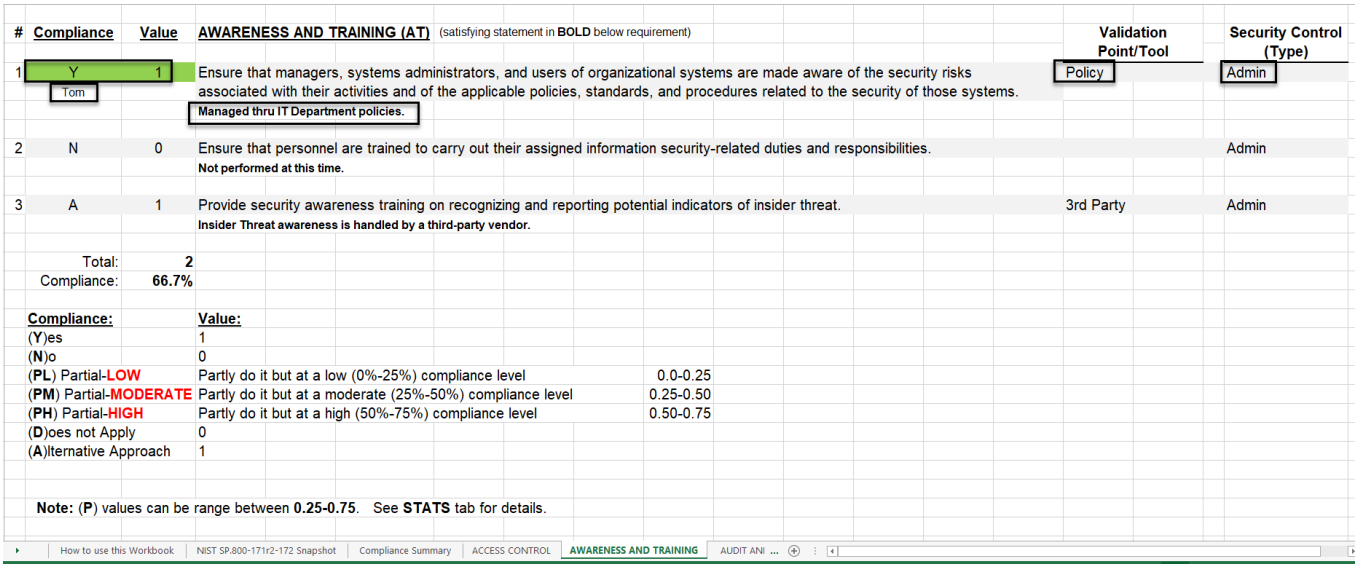
[7] This control family is not included in SP.800-53r5 but is unique to SP.800-172. Reference only.

2.4: Design

General Framework

Microsoft Excel was used to create the Security Assessment Workbook[1]. Control-families are placed in separate worksheets along with summaries for Assessment *Snapshot*, *Compliance*, and *Adversary Effects*[2].

Data entry is accomplished through individual Control Family worksheets (example: *Awareness and Training* below). Questions are drawn verbatim and directly from their NIST publications. Although only two pieces of information are necessary to satisfy the question (i.e., requirement); *Satisfaction of Requirement* and *Satisfying Statement*, other information (*Name*, *Validation Point/Tool*, *Security Control Type*) ensures a complete and comprehensive answer.



#	Compliance	Value	AWARENESS AND TRAINING (AT) (satisfying statement in **BOLD** below requirement)	Validation Point/Tool	Security Control (Type)
1	Y Tom	1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. **Managed thru IT Department policies.**	Policy	Admin
2	N	0	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. **Not performed at this time.**		Admin
3	A	1	Provide security awareness training on recognizing and reporting potential indicators of insider threat. **Insider Threat awareness is handled by a third-party vendor.**	3rd Party	Admin
	Total:	2			
	Compliance:	66.7%			

Compliance:	Value:	
(**Y**)es	1	
(**N**)o	0	
(**PL**) Partial-**LOW**	Partly do it but at a low (0%-25%) compliance level	0.0-0.25
(**PM**) Partial-**MODERATE**	Partly do it but at a moderate (25%-50%) compliance level	0.25-0.50
(**PH**) Partial-**HIGH**	Partly do it but at a high (50%-75%) compliance level	0.50-0.75
(**D**)oes not Apply	0	
(**A**)lternative Approach	1	

Note: (**P**) values can be range between **0.25-0.75**. See **STATS** tab for details.

How to use this Workbook | NIST SP.800-171r2-172 Snapshot | Compliance Summary | ACCESS CONTROL | AWARENESS AND TRAINING | AUDIT ANI ...

Formulas, calculated cells and cell references are used extensively to simplify data entry and avoid input or calculation error.

In addition to control requirements all worksheets contain the following variables:

- - Satisfaction of Requirement (Y/N/P/A/D) with corresponding value (0-1)
- - Satisfying Statement
  (maps to SP.800-172A ***Examine*** assessment method)
- - Name
  (maps to SP.800-172A ***Interview*** assessment method)
- - Validation Point/Tool (text)
  (maps to SP.800-172A ***Test*** assessment method)
- - Security Control-HIPAA Type (Administrative, Technical, Physical)
  {Healthcare sector only}

Note: SP.800-172 (only) *Enhanced* Security Requirements contain the following column/row variables:

- Assessment Methodology (*Examine*, *Interview*, *Test)*
- Depth & Coverage (*Basic*, *Focused*, *Comprehensive)*

See Appendix A for details.

[1] The Workbook is included as part of this book and can be downloaded from the Downloads Page.

[2] Snapshot, Compliance and Adversary Map worksheets display aggregate data pulled from control-family worksheets.

2.5: Variables

Variable: *COMPLIANCE* & *VALUE* (Figure 1)
Type: String or Text
Definition: Value expressing organizational compliance with and satisfaction of the security requirement. Numeric value is assigned to text value (e.g., Yes = 1) which is then used to calculate individual, group and statistical compliance.

The organization:
(**Y**) performs this task[1]
(**P**) partially performs this task
(**A**) uses an alternate approach to perform this task (that satisfies the requirement)
(**N**) does not perform this task
(**D**) this control requirement does not apply

Variable: VALUE
Depending on compliance, the following numerical values are automatically assigned:
Y or **A** = 1
P(L)(M)(H) = Low (.25), Medium (.50), High (.75) respectively
D or **N** = 0

#	Compliance	Value	ACCESS CONTROL (AC) (satisfying statement in BOLD below requirement)	Validation Point/Tool		Security Control (Type)
1	Y	1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Act.Dir (AD)	Tool 2	Admin
	Tom		**Role-based Access Control (RBAC).**	Tool 3		

Figure 1. Compliance (note: Value (0-1) is automatically entered depending on level-of-compliance)

Variable: *SATISFYING STATEMENT* (Figure 2)
Type: String or Text
Definition: a short but concise statement conveying how the (control) requirement is satisfied.

Normally, security assessments require detailed explanations[2] of policies and/or procedures in order to satisfy a particular security requirement. Such detail may require additional allocation of resources (i.e., time, staff & effort) to complete. The approach taken here is to provide a "trimmed" answer which nevertheless satisfies the requirement. For example, under ACCESS CONTROL, the question: (do you) "*Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)*"? A short, satisfying statement would be (yes) via "Role-based Access Control (RBAC)". The trimmed statement, *Role-based Access Control (RBAC)*, is placed in the cell directly below the control-requirement.

#	Compliance	Value	ACCESS CONTROL (AC) (satisfying statement in BOLD below requirement)	Validation Point/Tool		Security Control (Type)
1	Y	1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Act.Dir (AD)	Tool 2	Admin
	Tom		**Role-based Access Control (RBAC).**	Tool 3		

Figure 2. Satisfying Statement

Variable: *NAME* (Figure 3)
Type: String or Text
Definition: The person responsible for providing the Satisfying Statement. This value is normally placed in the cell directly below the Satisfaction of Requirement (Y, N) variable.

#	Compliance	Value	ACCESS CONTROL (AC) (satisfying statement in BOLD below requirement)	Validation Point/Tool		Security Control (Type)
1	Y	1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Act.Dir (AD)	Tool 2	Admin
	Tom		**Role-based Access Control (RBAC).**	Tool 3		

Figure 3. Name

Variable: *VALIDATION POINT/TOOL* (Figure 4)
Type: String or Text
Definition: a short, concise statement describing the tool, process or procedure used to satisfy the control requirement.

This information describes what application, utility, or process is used to satisfy the control requirement. Often, the same tool is used to satisfy multiple requirements or multiple requirements are satisfied by a single tool (example: an IDS[3] for network security).

#	Compliance	Value	ACCESS CONTROL (AC) (satisfying statement in BOLD below requirement)	Validation Point/Tool	Security Control (Type)
1	Y	1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Act.Dir (AD) Tool 2	Admin
	Tom		**Role-based Access Control (RBAC).**	Tool 3	

Figure 4. Validation Point/Tool

Variable: *SECURITY CONTROL/TYPE** **(Figure 5)**

This value directly references HIPAA's Security Rule which requires security controls to be categorized as *Administrative*, *Technical* or *Physical*. Most often, a security control has but a single categorization but there are instances where a control may encompass more than one. For example, establishing an operational incident-handling capability may be categorized as both an Administrative and Technical control.

#	Compliance	Value	ACCESS CONTROL (AC) (satisfying statement in BOLD below requirement)	Validation Point/Tool	Security Control (Type)
1	Y	1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Act.Dir (AD) Tool 2	Admin
	Tom		**Role-based Access Control (RBAC).**	Tool 3	

Figure 5. Security Control Type (note: applies to healthcare (HIPAA) sector only)

* this variable is only required for healthcare assessments.

[1] The term 'task' implies steps taken to satisfy the control requirement.

[2] The level of detail need only be sufficient to satisfy the security requirement. Nevertheless, more often than not extensive and detailed explanations are given.

[3] Intrusion Detection System (IDS)

2.6: Using the Assessment Workbook

In effect, the Security Assessment consists of two segments; worksheets containing questions (requirements) related to SP.800-171r2/172 Control Families (Figure 1) and worksheets containing Snapshot summary and Compliance evaluation (Figure 2). In addition there are several worksheets that contain useful reference information for completing the Assessment.

#	Requirement Satisfied?	Value	AWARENESS AND TRAINING (AT) (Satisfying statement in BOLD below requirement)	Validation Point/Tool		Security Control (Type) (HIPAA)
1	Y	1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. **Managed thru IT Department policies.**	Policy	Bulletins	Admin
2	N	0	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.			
3	N	0	Provide security awareness training on recognizing and reporting potential indicators of insider threat.			
	ENHANCED - SP.800-172					
4	N	0	Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training [at least annually] or when there are significant changes to the threat.			
5	N	0	Include practical exercises in awareness training for [users] that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.			

Questions in BLUE font are enhanced security requirements (NIST-SP.800-172)

Total: 1
Compliance: 20.0%

Req. Satisfied	Value:	
(Y)es	1	
(N)o	0	
(PL) Partial-LOW	Partly do it but at a low (0%-25%) compliance level	0.0-0.25
(PM) Partial-MODERATE	Partly do it but at a moderate (25%-50%) compliance level	0.25-0.50
(PH) Partial-HIGH	Partly do it but at a high (50%-75%) compliance level	0.50-0.75
(D)oes not Apply	0	
(A)lternative Approach	1	

Note: (P) values can be range between **0.25-0.75**. See **STATS** tab for details.

SP.800-172A

Assessment Method	Depth*	Coverage*
Examine	Comprehensive	Comprehensive
Interview	Focused	Focused
Test	Comprehensive	Comprehensive
Examine	Basic	Basic
Interview	Basic	Basic
Test	Basic	Basic

Note: *Depth* & *Coverage* values do not impact satisfaction value. See 'How to use this Workbook' tab for further details.

Figure 1. Control-Family (e.g., Awareness and Training) data entry worksheet

The Control Family worksheets are used for input and are the only worksheets requiring data. The *Requirement (Satisfied?)* field is the only required field whereas all others--Satisfaction Statement, Name, Validation Point/Tool, HIPAA Security Control (Type) and Assessment Method (for Depth and Coverage)--are optional (Figure 2).

SNAPSHOT

NIST SP.800-171r2 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations) [110 security-control requirements]
NIST SP.800-172* (Enhanced Security Requirements for Protecting Controlled Unclassified Information) [34 security-control requirements]
*In July, 2020, NIST renamed *Enhanced Security Requirements for Critical Programs and High Value Assets* (SP.800-171B) to *Enhanced Security Requirements for Protecting Controlled Unclassified Information* (SP.800-172)
Note: Questions in **BOLD** and **BOXED** at the bottom of each Control Family denotes *Enhanced* Security

Completed: 99/99/202X

NIST	#	Satisfied?	Control Family: ACCESS CONTROL (AC)
3.1.1	1	N	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
3.1.2	2	N	Limit system access to the types of transactions and functions that authorized users are permitted to execute.
3.1.3	3	N	Control the flow of CUI in accordance with approved authorizations.
3.1.4	4	N	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
3.1.5	5	N	Employ the principle of least privilege, including for specific security functions and privileged accounts.
3.1.6	6	N	Use non-privileged accounts or roles when accessing nonsecurity functions.
3.1.7	7	N	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
3.1.8	8	N	Limit unsuccessful logon attempts.
3.1.9	9	N	Provide privacy and security notices consistent with applicable CUI rules.
3.1.10	10	N	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
3.1.11	11	N	Terminate (automatically) a user session after a defined condition.
3.1.12	12	N	Monitor and control remote access sessions.
3.1.13	13	N	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
3.1.14	14	N	Route remote access via managed access control points.
3.1.15	15	N	Authorize remote execution of privileged commands and remote access to security-relevant information.
3.1.16	16	N	Authorize wireless access prior to allowing such connections.
3.1.17	17	N	Protect wireless access using authentication and encryption.
3.1.18	18	N	Control connection of mobile devices.
3.1.19	19	N	Encrypt CUI on mobile devices and mobile computing platforms.
3.1.20	20	N	Verify and control/limit connections to and use of external systems.
3.1.21	21	N	Limit use of portable storage devices on external systems.
3.1.22	22	N	Control CUI posted or processed on publicly accessible systems.
3.1.1e	23	N	**Employ dual authorization to execute critical or sensitive system and organizational operations.**
3.1.2e	24	N	**Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.**
3.1.3e	25	N	**Employ [secure information transfer solutions] to control information flows between security domains on connected systems.**

ASSESSMENT - SUMMARY			
No. of Questions\Completed\Pct.	110	110	100.0%
Compliance (SP.800 171r2) - **MEDIUM** Security			9.03%
No. of Questions\Completed\Pct.	144	144	100.0%
Compliance (SP.800 171r2-172) - **HIGH** Security			9.72%

	# Questions	
Cont.Fam	Medium	High
AC	22	25
AT	3	5
AU	9	9
CM	9	12
IA	11	14
IR	3	5
MA	6	6
MP	9	9
PS	2	4
PH	6	6
RA	3	10
SA	4	5
SC	16	20
SI	7	14
	110	144

Figure 2. Control-Family (e.g., Access Control (AC)) Snapshot

Information entered into each worksheet is then used as input for Snapshot and Compliance worksheets (**note:** Adversary Map data is manually entered and not considered essential for completion of the Assessment. See Appendix B for further information).

A closer view the Control-Family worksheet (Figure 1) shows incorporation of SP.800-172A assessment methods (Figure 3). Methods are used only to evaluate enhanced/High security requirements.

SP.800-172A		
Assessment Method	**Depth***	**Coverage***
Examine	Basic	Basic
Interview	Basic	Basic
Test	Basic	Basic
Examine	Comprehensive	Comprehensive
Interview	Comprehensive	Comprehensive
Test	Comprehensive	Comprehensive
Examine	Comprehensive	Comprehensive
Interview	Comprehensive	Comprehensive
Test	Comprehensive	Comprehensive
Note: *Depth* & *Coverage* values do not impact satisfaction value. See 'How to use this Workbook' tab for further details.		

Figure 3. Assessment Method matrix

In the context of a security assessment, *completion* is the extent to which all questions have been answered (i.e., satisfied). Given the number of questions in the assessment[1] the more complete it is the more accurate the results.

Compliance is defined as the extent an organization's security 'posture' is aligned with and satisfies individual requirements of SP.800-171r2 (Medium-security) or SP.800-171r2 and SP.800-172 (Enhanced/High-security). Compliance establishes whether or not, for a given security-control the Validation Tool maps to the requirement. This process is especially useful in identifying security requirements with either no associated tool or an insufficient one.

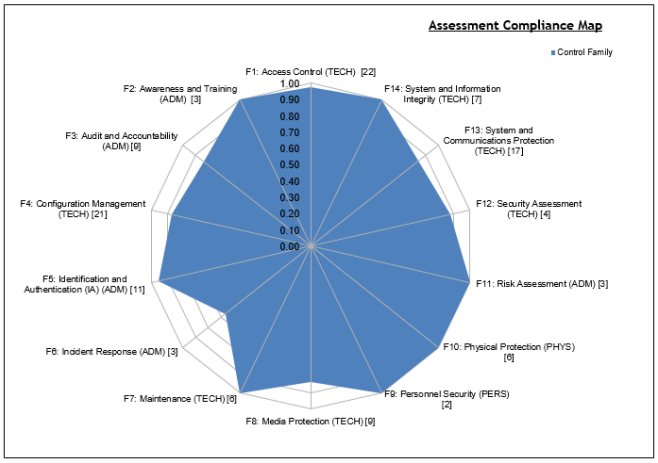
Point value and compliance percentage is computed for each control-requirement worksheet with results displayed at the bottom of each sheet (see Figure 1). As stated earlier, this information is used as reference for the Snapshot worksheet and as input for the Compliance worksheet. The Snapshot worksheet provides an aggregate view of all Control-Family responses as well as a summary of completion and compliance (Figure 2).

Compliance is summarized via the Compliance Summary worksheet (Figure 4). All values are pulled from the individual Control Family worksheets. Optional color-coding is used to aid readability.

NIST-SP.800-171r2 Compliance Summary
(Internal Use Only)

Compliance Score (%)
89.84%

	Questions whose answers are:					
	Y, A	P	N, D	Tot.	Value	Pctg.
F1: Access Control (TECH) [22]	21	1	0	0.5	21.5	98%
F2: Awareness and Training (ADM) [3]	3	0	0	0	3.0	100%
F3: Audit and Accountability (ADM) [9]	7	1	1	0.5	7.5	83%
F4: Configuration Management (TECH) [21]	15	5	1	2.5	17.5	88%
F5: Identification and Authentication (IA) (ADM) [11]	10	1	0	0.5	10.5	95%
F6: Incident Response (ADM) [3]	2	0	1	0	2.0	67%
F7: Maintenance (TECH) [6]	6	0	0	0	6.0	100%
F8: Media Protection (TECH) [9]	7	1	1	0.5	7.5	83%
F9: Personnel Security (PERS) [2]	2	0	0	0	2.0	100%
F10: Physical Protection (PHYS) [6]	6	0	0	0	6.0	100%
F11: Risk Assessment (ADM) [3]	3	0	0	0	3.0	100%
F12: Security Assessment (TECH) [4]	3	1	0	0.5	3.5	88%
F13: System and Communications Protection (TECH) [17]	13	1	3	0.5	13.5	84%
F14: System and Information Integrity (TECH) [7]	7	0	0	0	7.0	100%
Total:	105	11	7	123	110.5	90%



About
This Security Assessment consists of 123 questions covering 14 security control *Families*. Questions are derived exclusively from NIST-SP.800-171r2 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations), published June, 2019. SP.800-171r2 questions reference and align with NIST Cybersecurity Framework (CSF), v1.1 and NIST SP.800.53r5 Security & Privacy Control Catalog. These documents align with HIPAA/Security Rule guidance for CIA of protected health information (PHI). The purpose of this assessment is to determine level-of-compliance with current/emerging industry-domain guidance for information and cyber-physical information security.

Directions: Complete the map by deducting the number or answered (i.e., completed) questions from the total for each section. Place the number answered "yes" in the 'Yes' column and the number of "partial" or "alternative" in the 'P, A' column. Together, the number can equal the number of questions in each respective section (highlighted in brackets []). 'Yes' and 'Alternative' answers have a value of 1, and 'Partial' answers .05. Total column is sum of both columns and is converted to a percentage. The goal is to complete as much of the map as possible with 80%-100% an acceptable range for compliance.

Values are computed as follows: **Yes**=1, **Alternative Method**=1, **Partial**=.05, **No**=0, **Does Not Apply**=0
Note: Cells highlighted in yellow or dark gray are calculated fields

Figure 4. Individual and aggregate Control-Family compliance summary

A data table and radar[2] (aka spider) chart provide tabular and graphical depiction of each Control Family's value for aggregate compliance. The radar chart is especially useful for viewing deficiencies and areas which need to be addressed.

An acceptable individual control-family or aggregate compliance level is left to the discretion of the organization as there is no published or uniformly agreed upon standard.

Regardless of threshold, compliance provides an organization with an idea of how well its security posture compares to established or recommended industry-standards.

[1] SP.800-171r2 contains 110 control requirements and SP.800-172 has 34. Both publications comprise a total of 144 security-control requirements.

[2] A radar chart compares the values of three or more variables relative to a central point. It's useful when you cannot directly compare the variables and is especially great for visualizing performance analysis or survey data.

CHAPTER OVERVIEW

3: Security Assessment using SP.800-213 and SP.800-213A

3.1: Introduction

Author's Note

On 11/29/2021, NIST published Special Publication (SP) 800-213, *IoT Device Cybersecurity for the Federal Government*. This publication builds upon and expands considerations for Internet of Things (IoT) security initially published[1] in NISTIR publications 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* and 8259A, *IoT Device Cybersecurity Capability Core Baseline*.

As stated in SP.800-213/213A Abstract(s):

This publication contains background and recommendation to help organizations consider how an IoT device they plan to acquire can integrate into a system. IoT devices and their support for security controls are presented in the context of organizational and system risk management[2].

As has been stated throughout this book, specific guidance for conducting and completing a security assessment has been directed at the healthcare sector but the principles and process described within can be equally applied to any sector or industry.

[1] NISTIR 8259 series published June, 2019.

[2] NIST-SP. 800-213. [ii]

According to Cisco Internet Business Solutions Group the 'Internet of Things' (IoT) began sometime between 2008 and 2009 when the number of "things or objects" connected to the internet exceeded the number of people connected.

Published references to the *Medical Internet of Things* (MIoT) most likely started between 2012 and 2013. In 2012, the Government Accounting Office (GAO) recommended in the August edition of its *Highlights* report to Congress[1] that the FDA should "develop and implement a plan expanding its focus on information security risks." Indeed, in 2013[2] the Food and Drug Administration (FDA) issued medical device manufacturers guidance for the cybersecurity of medical IoT devices[3] which represented the agency's "current thinking on this topic."

The Healthcare sector has been quick to incorporate MIoT into clinical operations as such use offers greater efficiency, improved operations, cost savings and most importantly, improved patient outcomes. Examples where MIoT are employed include blood pressure and glucose level monitoring, pulse oxymeters, weight/BMI scales, thermometers, spirometers, and EKG monitoring.

The key to success of MIoT (in fact, all IoT) is internet-connectivity and the ability of MIoT devices to transmit (patient) information.

In December 2020, President Trump signed into law the *IoT Cybersecurity Improvement Act of 2020*. This law, in part, directs the National Institute of Standards and Technology (NIST) to take steps for the increased cybersecurity of IoT. In accordance with this law, in late November NIST published Special Publication (SP) 800-213 (*IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*). Although written for government agencies the guidance contained in NIST Special Publications can be used by non-government organizations as well and SP.800-213 is no exception.

Based on NIST guidance, a qualitative framework for assessing IoT (and by extension MIoT) cybersecurity and privacy protection is possible. Using *Expectations* for MIoT cybersecurity and privacy protection outlined in NIST.IR 8228 (and associated publications[4]) a set of criteria is used to assess security and compliance, and in turn, evaluate weakness or (data) exposure which a MIoT device may pose to a healthcare organization's IT environment. Moreover, such evaluation is crucial for complying with HIPAA/HITECH regulations governing the Confidentiality, Integrity and Availability (CIA) of Protected Health Information (PHI).

How can healthcare organizations (from small Practices to large HDOs[5] evaluate adherence to the cybersecurity and privacy protection of MIoT devices used in clinical settings? This discussion suggests an approach for such evaluation which make it possible to quantitatively assess cybersecurity and privacy protection, and determine relative compliance with recommended standards. It further allows organizations to evaluate the level of risk a MIoT device poses to IT systems and to determine whether or not to permit its use in healthcare/IT environments.

The current state of IoT/MIoT cybersecurity and privacy protection using historical and current industry guidance & best-practices; recommendations by federal agencies; NIST publications; and federal laws are reviewed for similarities and differences which are

then incorporated into a Security Assessment.

Variations in data transmission and storage between IoT/MIoT devices and “traditional” (or classic) Information Technology (IT) hardware are presented along with challenges IoT/MIoT pose to cybersecurity and privacy protection.

Finally, a process for evaluating cybersecurity and privacy protection via Security Assessment is offered along with enhancements for validating results. Doing so demonstrates general compliance with both NIST guidance and HIPAA/HITECH requirements.

---

[1] GAO Highlights, GAO-12-816.

[2] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. Guidance for Industry and Food and Drug Administration Staff. First draft published June 14, 2013. Food and Drug Administration, et al.

[3] It should be noted that the FDA issued guidance for “…Software Contained in Medical Devices” in May, 2005, however, this publication pre-dated IoT and concerned itself with embedded software.

[4] NIST Cybersecurity Framework (CSF), NISTIR 8259 series, SP.800-53r5 (Security and Privacy Controls for Information Systems and Organizations) and SP.800-213/213A (IoT Device Security Guidance for the Federal Government).

[5] Health Delivery Organization (HDO)

3.2: Governance and Oversight

MIoT GOVERNANCE & OVERSIGHT

By definition, MIoT devices are IoT devices used for a specialized purpose (healthcare). Specialization notwithstanding, MIoT devices are subject to the same cybersecurity and privacy protection requirements as non-MIoT or IoT devices. According to the Food and Drug Administration (FDA), cybersecurity is a shared responsibility between the FDA and "device manufacturers, hospitals, healthcare providers, patients, security researchers, and other government agencies including the U.S. Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) and U.S. Department of Commerce." [1]

U.S. FOOD AND DRUG ADMINISTRATION (FDA)

The Department of Health and Human Services (HHS), Food and Drug Administration (FDA) is responsible for medical device oversight. According to the General Accounting Office (GAO), the FDA is responsible "for ensuring the safety and effectiveness of medical devices in the United States". [2]

In 2012, the GAO recommended in its August *Highlights* report to Congress that the FDA should "develop and implement a plan expanding its focus on information security risks."

Pursuant to its responsibility the FDA has published guidance for both Premarket (2014) and Postmarket (2016) management of cybersecurity in MIoT devices.

In 2014, FDA Center for Devices and Radiological Health, released *Content of Pre-Market Submissions for the Management of Cybersecurity in Medical Devices* (FDA 1825). This publication provides guidance for Industry, and FDA staff. Though 'Internet of Things' is not specifically mentioned in the document--understandable given that MIoT devices were in the very early stages of being applied to the Healthcare sector—it nevertheless recommends that "medical device manufacturers address cybersecurity during the design and development of the medical device, as this can result in more robust and efficient mitigation of patient risks". Cybersecurity areas addressed included identification of threats and vulnerabilities; assessment of the impact of threats on device functionality and end users\patients; assessment of the likelihood of threat\vulnerability occurring; determination of risk levels; and assessment of residual risk and risk acceptance criteria. Moreover, the recommendations specifically cite NIST Cybersecurity Framework categories *Identify*, *Protect*, *Detect*, *Respond* and *Recover*.

In 2016, FDA Center for Devices and Radiological Health, released *Postmarket Management of Cybersecurity in Medical Devices*. Similar to FDA 1825, this publication clarifies postmarket recommendations for manufacturers to follow relative to identifying, monitoring and addressing cybersecurity vulnerabilities and exploits as "part of their postmarket management of medical devices"[3].

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) GUIDANCE

In 2019, the NIST released Internal Report[4] (IR) NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*.

In 2020, NISTIRs 8259(A)(B)(C)(D) were released as supplementary/complementary Guides for IoT cybersecurity. These publications provided guidance to IoT device manufacturers (8259/8259A); guidance for non-technical support capabilities (8259B); guidance for Core security baselines (8259C); and guidance for creating a Profile for IoT Baselines (8259D) for the federal government.

Pursuant to passage of federal law governing IoT cybersecurity[5], in December, 2020 NIST published SP.800-213/213A, *IoT Device Cybersecurity Guidance for the Federal Government*. These publications, updated in November, 2021, expand upon and supersede criteria outlined in the NISTIR series. SP.800 213/213A provides specific IoT cybersecurity requirements and references several NIST Guides which have cross-application to HIPAA and HITECH requirements. Among them: NIST Cybersecurity Framework and SP.800-53r5 (Security & Privacy Control Catalog). Collectively, these Guides provide the basis for a framework which can be used to determine IoT/MIoT compliance with cybersecurity and privacy protection.

SP.800-213A, *IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog* defines seven (7) distinct security Capabilities for IoT devices:

- Identification
- Configuration
- Protection
- Logical Access
- Software Update

- Cybersecurity State Awareness
- Device Security

In turn, each Capability contains one or more sub-Capabilities (e.g., Actions based on Device Identity). For each, sub-Capability there may be one or more Requirements (e.g., Ability to perform actions that can occur based on or using the identity of the device) which satisfy the sub-Capability. Finally, each Requirement may contain one or more sub-Requirements (e.g., Ability to hide IoT device identity from non-authorized entities) which satisfy the Requirement.

In addition to FDA and NIST guidance the private sector has added its perspective to MIoT cybersecurity and privacy protection. In 2018, the Medical Device Innovation Consortium[6] (MDIC), a non-profit, public-private partnership published *Medical Device Cybersecurity Report*: *Advancing Coordinated Vulnerability Disclosure* with the purpose of "coordinated vulnerability disclosure (CVD) policies by medical device manufacturers".

FEDERAL LAWS AFFECTING MIoT

New laws were enacted in 2020 and 2021 that will have an important impact on MIoT cybersecurity and privacy protection.

On December 4, 2020, the *IoT Cybersecurity Improvement Act of 2020*[7] was signed into law by President Donald Trump. This law required, in part, that NIST develop standards and guidelines for the federal government to follow governing IoT devices used or controlled by a government agency. As stated earlier, NIST guidance can be readily adapted by private-sector companies and organizations.

On January 5, 2021, President Trump signed into law an amendment to the *Health Information Technology for Economic and Clinical Health Act* (HITECH). HR 7898, otherwise known as the *HIPAA Safe Harbor* provision directs HHS to factor, in part, an organization's use of industry-standard cybersecurity practices during the previous twelve (12) months when investigating suspected data breaches or other violations. The amendment is meant to encourage healthcare providers and organizations to use NIST best-practices when formulating their cybersecurity and privacy protection strategies.

---

[1] GAO Highlights, GAO-12-816., 3

[2] GAO Highlights, GAO-12-816., 20

[3] Postmarket Management of Cybersecurity in Medical Devices. Guidance for Industry and Food and Drug Administration Staff. 2016. Food and Drug Administration. Department of Health and Human Services. 18

[4] NISTIR (Internal or Interagency Report). Reports of research findings, including background information for FIPs and SPs. Source: https://csrc.nist.gov/publications/. Retrieved: 03/22/21.

[5] Internet of Things Cybersecurity Act of 2020. Signed into law on December 04, 2020.

[6] https://mdic.org/

[7] H.R. 1668, Public Law 116-207. The IoT Cybersecurity Act of 2020 was first introduced into Congress in 2017.

3.3: Challenges to Assessing IoT-MIoT

Healthcare is governed by the provisions of HIPAA and HITECH. Both contain specific regulations and\or requirements for the protection of ePHI and other sensitive information. Any process, system or device used to create, transmit or store ePHI is subject to these provisions.

For healthcare organizations and providers MIoT devices represent several cybersecurity and privacy protection challenges. Central to which is that MIoT devices do not behave, operate, or perform in the same manner as traditional[1] IT devices. This difference is due to a MIoT device's core functions *Sensing* (retrieving and transmitting information about the real world and transmitting it) and *Actuating* (making changes to the physical world). Some of the differences between MIoT and traditional IT include:

1. The ability to configure, update and monitor
2. Lack of transparency (black box problem)
3. Compatibility with existing Infrastructure
4. Information security (CIA)
5. Third-party access

The ability to configure, update and **monitor** means, at a minimum, having access to the MIoT device in order to perform routine and as-needed management functions such as access control (e.g., passwords), software updates (i.e., patch management) and log review. Due to manufacture design and production this level of access may not be available or even possible. It may not even be possible to know, to a reasonable degree of certainty, if the MIoT device is functioning properly or at all.

Lack of transparency (black box problem) is an issue with some MIoT devices due to their design and manufacture. Such devices do not allow insight into their configuration, operational settings or performance/activity logs. Lack of transparency prevents normal or routine cybersecurity and privacy protection oversight, and introduces risk into an IT environment since the state of compliance (with HIPAA/HITECH regulations) is unknowable.

Compatibility with existing Infrastructure may cause concern for established Datacenters and IT networks. Since MIoT devices may operate and function differently than traditional IT devices such difference can result in incompatibility with systems that were not designed for MIoT integration. In turn, MIoT devices may require new management systems for proper operation and oversight with IT Departments finding it necessary to add resources (staff & skills or external services) to manage MIoT deployment within their networks.

Information Security (CIA) is a core tenant of HIPAA. CIA means taking appropriate steps to protect the Confidentiality, Integrity and Availability of protected health information (PHI). If a MIoT device stores data (not all do) it is critical that it be protected—depending on whether or not said information is PHI or CUI2--using cryptography or some other means of data protection. 'Black-box' devices or devices without any type of access or insight into their operation or status introduces significant risk in the event of exploit or compromise.

Third-party access is of concern for MIoT devices which permit no end-user access to their configuration settings or operational status (only third-parties). Such "unmanaged" devices may prevent real-time access during operational error or failure with access delayed further if the third-party is unavailable. It may also prevent those responsible from properly gauging network or operational status of a MIoT device when a software or firmware update is required, device End-of-Life (EOL) is reached, or for other routine management and maintenance functions. In addition, a manufacturers **Software Bill of Materials** (SBOM) may be unavailable to a healthcare provider that is considering using MIoT devices in its clinical setting(s).

[1] Or "classic" IT devices such as routers, switches, servers, etc…

[2] Confidential but Unclassified Information (CUI). Reference NIST.SP-800-171 & NIST.SP-800-172.

3.4: Using NIST SP.800-213A Capabilities for MIoT Security Assessment

Using NIST guidance (augmented by federal law), FDA guidance and private-sector recommendations a simple framework can be created for assessing the level of cybersecurity and privacy protection a MIoT device possesses. By using the framework the level of overall compliance (with recommended standards) can be obtained which, in turn, can be used to determine acceptable levels of security and risk.

SP.800-213A, *IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog* defines seven (7) distinct security Capabilities for IoT devices:

- Identification
- Configuration
- Protection
- Logical Access
- Software Update
- Cybersecurity State Awareness
- Device Security

In turn, each Capability contains one or more sub-Capabilities (e.g., Actions based on Device Identity). For each, sub-Capability there may be one or more Requirements (e.g., Ability to perform actions that can occur based on or using the identity of the device) which satisfy the sub-Capability. Finally, each Requirement may contain one or more sub-Requirements (e.g., Ability to hide IoT device identity from non-authorized entities) which satisfy the Requirement (Figure 1).

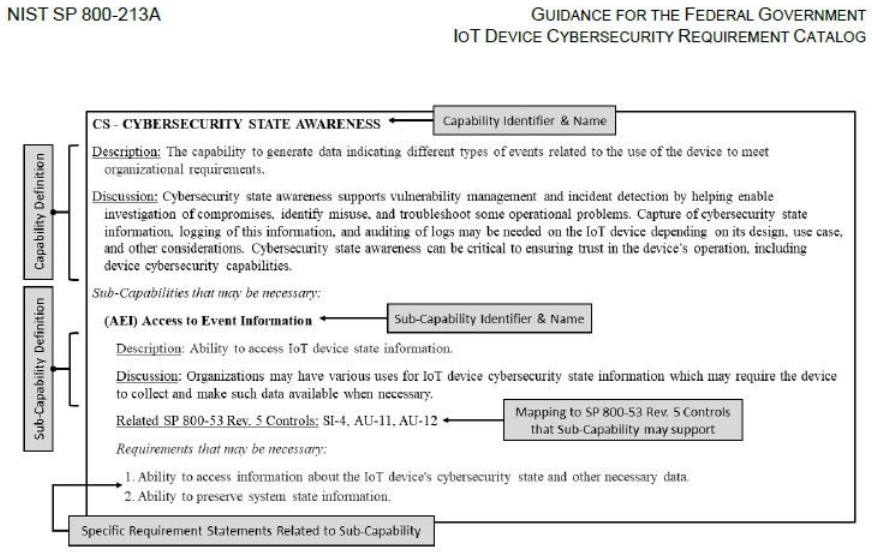


Figure 1: Capability and Sub-Capability Structure

In addition, references to NIST Cybersecurity Framework and NIST.SP 800-53r5 (Security Control Catalog) are provided along with organizational Implications.

All told, SP.800-213A categorizes specific requirements as follows:

- 7 Capabilities
- 39 sub-Capabilities
- 257 Requirements & sub-Requirements

In terms of detail, *Logical Awareness* and *Cybersecurity State Awareness* Capabilities comprise 58% of the total requirements.

By assessing relative compliance with Requirements overall compliance can be assessed and quantified at the Capability & sub-Capability levels and further granulated at Requirement\sub-Requirement levels. This information can then be used to a) evaluate

risk, b) identify MIoT weaknesses or vulnerabilities, c) gauge the level of IT management required and d) evaluate whether or not to allow the MIoT device into a network.

3.5: Evaluation Process

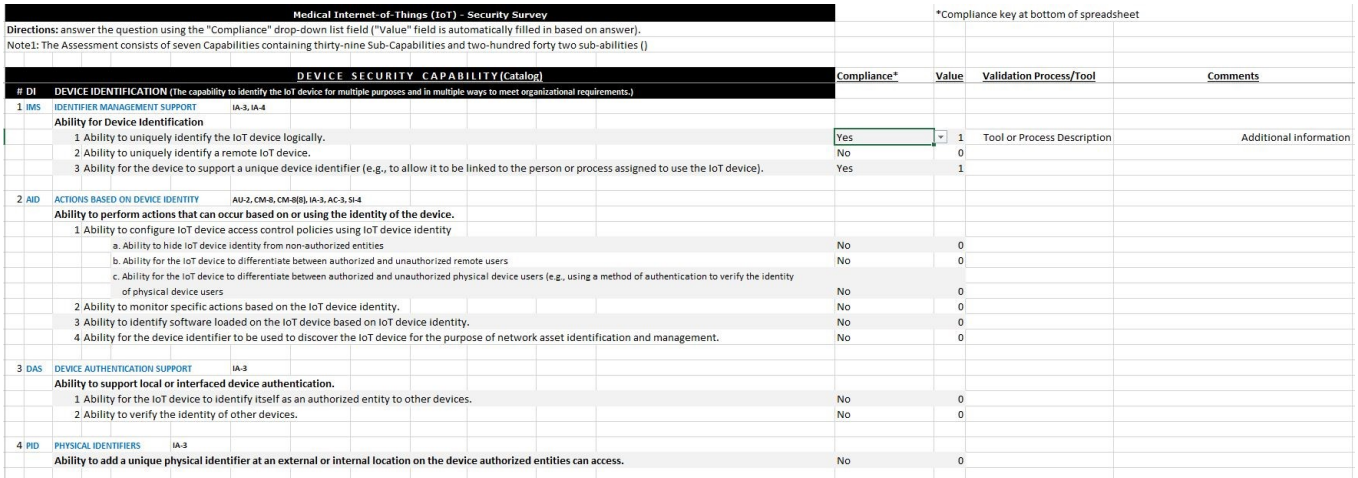
The evaluation process consists of determining compliance (with SP.800-213A Capabilities) and assessing the level of risk (acceptable, correctable or unacceptable) a MIoT device presents to a healthcare organization's IT environment. The process should also include evaluation with HIPAA/HITECH requirements for the protection of PHI. *Compliance-with-Requirement* should be completed by either the MIoT device manufacturer or vendor on behalf of the healthcare provider considering its use. An assessment can be completed by the healthcare provider but may be inaccurate—through no fault of the healthcare provider--unless supporting or corroborating evidence (or documentation) is provided by manufacturer or vendor.

3.6: Methodology - Design and Variables

> **Note**
>
> The MIoT Assessment tool is designed in a similar manner as the Security Assessment using NIST.SP 800-171r2/172.

Microsoft Excel was used to create the MIoT Security Assessment Workbook (Figure 2). The workbook utilizes NIST SP.800-213A Capabilities, sub-Capabilities, Requirements and sub-Requirements to establish a quantitative framework for assessing MIoT cybersecurity and privacy protection compliance. In addition to specific Requirements the workbook provides references to associated NIST publications (SP.800-53r5) for each requirement.

The assessment process consists of determining compliance with the *Requirement/sub-Requirement*, and providing proof of compliance via validation process or tool (Figure 1).



Medical Internet-of-Things (IoT) - Security Survey

*Compliance key at bottom of spreadsheet

Directions: answer the question using the "Compliance" drop-down list field ("Value" field is automatically filled in based on answer).

Note1: The Assessment consists of seven Capabilities containing thirty-nine Sub-Capabilities and two-hundred forty two sub-abilities ()

#	DI	DEVICE SECURITY CAPABILITY (Catalog)	Compliance*	Value	Validation Process/Tool	Comments
1	IMS	IDENTIFIER MANAGEMENT SUPPORT IA-3, IA-4				
		Ability for Device Identification				
		1 Ability to uniquely identify the IoT device logically.	Yes	1	Tool or Process Description	Additional information
		2 Ability to uniquely identify a remote IoT device.	No	0		
		3 Ability for the device to support a unique device identifier (e.g., to allow it to be linked to the person or process assigned to use the IoT device).	Yes	1		
2	AID	ACTIONS BASED ON DEVICE IDENTITY AU-2, CM-8, CM-8(8), IA-3, AC-3, SI-4				
		Ability to perform actions that can occur based on or using the identity of the device.				
		1 Ability to configure IoT device access control policies using IoT device identity				
		a. Ability to hide IoT device identity from non-authorized entities	No	0		
		b. Ability for the IoT device to differentiate between authorized and unauthorized remote users	No	0		
		c. Ability for the IoT device to differentiate between authorized and unauthorized physical device users (e.g., using a method of authentication to verify the identity of physical device users	No	0		
		2 Ability to monitor specific actions based on the IoT device identity.	No	0		
		3 Ability to identify software loaded on the IoT device based on IoT device identity.	No	0		
		4 Ability for the device identifier to be used to discover the IoT device for the purpose of network asset identification and management.	No	0		
3	DAS	DEVICE AUTHENTICATION SUPPORT IA-3				
		Ability to support local or interfaced device authentication.				
		1 Ability for the IoT device to identify itself as an authorized entity to other devices.	No	0		
		2 Ability to verify the identity of other devices.	No	0		
4	PID	PHYSICAL IDENTIFIERS IA-3				
		Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access.	No	0		

Figure 1: Validation Tool\Survey

SURVEY VARIABLES

Variables are *Compliance(value), Validation Process/Tool and Comments:*

Compliance	Value	Definition
Yes	1	The MIoT device complies with the Requirement\sub-Requirement
No	0	The MIoT device does not comply with the Requirement\sub-Requirement
Does Not Apply	1	Requirement\sub-Requirement does not apply to the device (requires explanation)
Alternate Approach	1	An alternate approach is used to comply with the Requirement\sub-Requirement
Unknown	0	it is unknown if compliance with Requirement\sub-Requirement is possible or available

Numerical values (0-1) are automatically added to the value column based on compliance value. Values are summed and used to determine overall level of MIoT cybersecurity and privacy protection compliance (with SP.800-213A Capabilities).

PROOF-OF-COMPLIANCE/VALIDATION PROCESS/TOOL

This variable represents a process, procedure or tool (manual or automated) which is used as auditable proof or evidence that the *Requirement* is being satisfied.

For example, for DEVICE IDENTIFICATION/Identifier Management Support: *Ability to uniquely identify the IoT device logically* the validation process may be a short statement such as “device ID/SN can be read by IT Asset Management System” with a tool reference to *ABC Asset Management* program or application[1] Validation is to provide sufficient supplementary or complementary information proving that the *Requirement* is being met.

COMMENTS

This variable provides for additional information.

[1] Short, concise statements are preferred for clarity and readability.

3.7: Using the Assessment Workbook

Once the MIoT assessment questionnaire is complete its information is then used to compute individual and overall compliance with SP.800-213A Capabilities and Requirements in both numerical and graphic (radar or spider chart) formats (Figure 1). This view allows evaluators to identify areas of weakness or vulnerability and to determine the level of cybersecurity and privacy protection when considering the use of a MIoT device in their network environment.

Summary of SP.800-213A Survey\Questionnaire responses

Group compliance is the sum of Requirements\sub-Requirements divided by the number of sub-Capabilities

#	Capability\Sub-Capability		Compl.	
	DI	DEVICE *IDENTIFICATION* (The capability to identify the IoT device for multiple purposes and in multiple ways to meet organizational requirements.)		
1	IMS	IDENTIFIER MANAGEMENT SUPPORT	67%	
2	AID	ACTIONS BASED ON DEVICE IDENTITY	0%	
3	DAS	DEVICE AUTHENTICATION SUPPORT	0%	Group Compliance: **17%**
4	PID	PHYSICAL IDENTIFIERS	0%	
	DC	DEVICE *CONFIGURATION* (The capability to configure the IoT device through logical and/or physical interfaces to meet organizational requirements.)		
5	PRV	LOGICAL ACCESS PRIVILEGE CONFIGURATION	100%	
6	AUT	AUTHENTICATION AND AUTHORIZATION CONFIGURATION	0%	
7	INT	INTERFACE CONFIGURATION	0%	Group Compliance: **23%**
8	DSP	DISPLAY CONFIGURATION	0%	
9	CTL	DEVICE CONFIGURATION CONTROL	14%	
	DP	DATA *PROTECTIO* N (The capability to protect IoT device data to meet organizational requirements.)		
10	CRY	CRYPTOGRAPHY CAPABILITIES AND SUPPORT	40%	
11	KEY	CRYPTOGRAPHIC KEY MANAGEMENT	0%	
12	STO	SECURE STORAGE	0%	Group Compliance: **10%**
13	STX	SECURE TRANSMISSION	0%	
	LA	*LOGICAL ACCESS* TO INTERFACES (Ability to require authentication to, and/or identification of, the IoT device, and to establish authentication and identification configuration and display requirements.)		
14	AUN	AUTHENTICATION SUPPORT	20%	
15	ACF	AUTHENTICATION CONFIGURATION	0%	
16	USE	SYSTEM USE NOTIFICATION SUPPORT	0%	
17	AUZ	AUTHORIZATION SUPPORT	0%	
18	AIM	AUTHENTICATION & IDENTITY MANAGEMENT	0%	Group Compliance: **2%**
19	ROL	ROLE SUPPORT & MANAGEMENT	0%	
20	LDU	LIMITATIONS ON DEVICE USAGE	0%	
21	XCN	EXTERNAL CONNECTIONS	0%	
22	IFC	INTERFACE CONTROLS	0%	

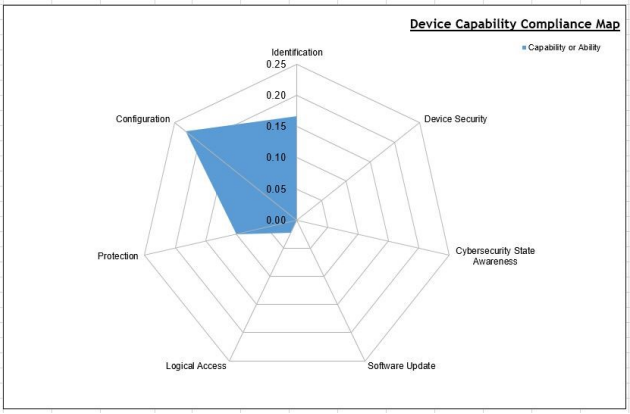


Figure 1: Compliance table and spider-view Chart

A data table and radar[1] (aka spider) chart provide tabular and graphical depiction of each *Requirement/sub-Requirement* value for aggregate compliance. A radar chart is especially useful for a birds-eye view (BEV) of deficiencies as well as highlighting areas which need to be addressed.

An acceptable compliance level is left to the discretion of the evaluator or organization as there is no published standard (although 75% or better is normally considered acceptable). Acceptable levels, however, can be designated for both individual *Requirements/sub-Requirements* and aggregate levels.

Regardless of threshold, compliance provides an organization with an idea of how well a MIoT device under consideration compares to established or recommended industry-standards. It is also used for determining the degree of risk (the MIoT represents) and ultimately whether or not its use is acceptable to a healthcare provider or organization.

[1] A radar chart compares the values of three or more variables relative to a central point. It's useful when you cannot directly compare the variables and is efficient for visualizing performance analysis or survey data.

3.8: Advantages and Benefits of Using NIST SP.800-213 and SP.800-213A for MIoT Assessment

1. SP.800-213A Capabilities, sub-Capabilities, Requirements\sub-Requirements can be used to evaluate MIoT security in alignment with HIPAA\HITECH requirements. At present, there are few assessments designed specifically to evaluate MIoT cybersecurity risk and\or privacy protection to such as extent as outlined in SP.800-213A.
2. Use of SP.800-213A Requirements\sub-Requirements can help protect the physical *Device;* its *Data* and data *Privacy* in order to evaluate security and risk[1].
3. The security assessment approach offered through SP.800-213A is easy to use, flexible, repeatable, and employs current industry Best-Practices and guidance for both MIoT manufacturer and healthcare organization.
4. The use of NIST SP.800-213A adheres to the intent of HITECH\HIPAA 'Safe Harbor' provision which encourages and incentivizes healthcare providers and organizations to use NIST publications and Best-Practice guidance when considering Cybersecurity and Privacy Protection programs.
5. Employing NIST SP.800-213A Requirements\sub-Requirements suggest an assessment process and methodology that is adaptable to non-federal sectors, and which can be used for regulatory and\or legal compliance.

Healthcare providers (i.e., Covered Entities) are mandated by HIPAA and HITECH to protect the Confidentiality, Integrity and Availability (CIA) of Electronic Protected Health Information (ePHI). This requirement extends to technology providers and Business Associates (BA) who directly support (healthcare) providers and use MIoT devices to satisfy this purpose.

SP.800-213A can be used to evaluate MIoT device compliance with other cybersecurity best practices relative to Device, Data and Privacy protection. Moreover, SP.800-213A associates its requirements to other NIST publications governing IoT and Cybersecurity including NIST's Cybersecurity Framework and SP.800-53r5 (Security Control Catalog).

Finally, SP.800-213A can be used to create a documented history of compliance. Such history can serve as a guide for healthcare organizations when considering changes to technology and/or network environments.

[1] Risk mitigation tiers are REDUCE, AVOID, ACCEPT and TRANSFER.

4: VI. Assessment Workbook Downloads

- How-To use Security and MIoT Assessment Workbooks (User Guide)
- NIST-SP.800-171r2-172 - Cybersecurity Assessment Workbook for Information Technology (IT) [Controlled Unclassified Information (CUI)-V3]
- NIST-SP.800-213A-IoT (Operational Technology\OT)-Cybersecurity Assessment Workbook-V2

References

Information Security (IS)

1. *Framework for Improving Critical Infrastructure Cybersecurity*. (2018). US Department of Commerce, National Institute of Standards and Technology.
2. *Health Insurance Portability and Accountability Act of 1996*. Pub. L. 104-191. Stat. 1936. HIPAA. Retrieved: https://www.govinfo.gov/content/pkg/...104publ191.pdf
3. *Health Information Technology for Economic and Clinical Health Act*. Pub. L. 111-5. Stat. 13001. (2019). HITECH. Retrieved: https://www.hhs.gov/sites/default/fi.../hitechact.pdf
4. *Minimum Security Requirements for Federal Information and Information Systems.* Federal Information Processing Standards Publication (FIPS) 200. (2006). US Department of Commerce, National Institute of Standards and Technology.
5. NIST Special Publication 800-53r5: *Security and Privacy Controls for Information Systems and Organizations.* (2017). US Department of Commerce, National Institute of Standards and Technology.
6. Ross, R., Pillitteri, V., Dempsey, K., Riddle, M. and Guissanie, G. (2019). NIST Special Publication 800-171r2: *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.* US Department of Commerce, National Institute of Standards and Technology.
7. Ross, R., Pillitteri, V., Guissanie, G., Wagner, R., Graubart, R. and Bodeau, D., (2020). NIST Special Publication 172: Enhanced Security Requirements for *Protecting Controlled Unclassified Information. A Supplement to NIST Special Publication 800-171*. US Department of Commerce, National Institute of Standards and Technology.
8. Ross, R., Pillitteri, V., Guissanie, G., Wagner, R., Graubart, R. and Bodeau, D., (2020). NIST Special Publication 172A: *Assessing Enhanced Security Requirements for Controlled Unclassified Information*. US Department of Commerce, National Institute of Standards and Technology.
9. Federal Information Processing Standards Publication (FIPS) 199. *Standards for Security Categorization of Federal Information and Information Systems.* (2004). US Department of Commerce, National Institute of Standards and Technology.

Operational Security (OS)

1. *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. Guidance for Industry and Food and Drug Administration Staff (First Draft)*. (2014). Department of Health and Human Services. Food and Drug Administration, 3
2. *Cybersecurity Safe Harbor provision*. Amendment to Health Information Technology for Economic and Clinical Health Act (HITECH), (2021). 42 USC 17931 §13412. Public Law 116-321.
3. *FDA Should Expand Its Consideration of Information Security for Certain Types of Devices*. (2012). General Accounting Office. GAO-12-816 Highlights, Medical Devices.
4. *Framework for Improving Critical Infrastructure Cybersecurity*. (2018). US Department of Commerce. National Institute of Standards and Technology.
5. Health Information Technology for Economic and Clinical Health Act. Pub. L. 111-5. Stat. 13001. (2009). HITECH. Retrieved from: https://www.hhs.gov/sites/default/fi.../hitechact.pdf
6. *Health Insurance Portability and Accountability Act of 1996*. (1996). Pub. L. 104-191. Stat. 1936. HIPAA. Retrieved from: https://www.govinfo.gov/content/pkg/...104publ191.pdf
7. *Internet of Things Cybersecurity Improvement Act of 2020*. H.R. 1668. (2020). Public Law 116-207. United States Congress.
8. *Medical Device Cybersecurity Report: Advancing Coordinated Vulnerability Disclosure. Medical Device Innovation Consortium*. (2018). Retrieved from: https://mdic.org/event/mdicx-cyberse...ty-disclosure/
9. *Medical Device Cybersecurity: What You need to Know.* (2020). Retrieved from: https://www.fda.gov/consumers/consum...-you-need-know
10. *Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health.* (2018). U.S. Food and Drug Administration. FDA-2018-N-1315.
11. NIST Special Publication (SP) 800-213: *IoT Device Cybersecurity for the Federal Government: Establishing IoT Device Cybersecurity Requirements.* (2021). US Department of Commerce. National Institute of Standards and Technology, 11.
12. NIST Special Publication (SP) 800-213A: *IoT Device Cybersecurity for the Federal Government: IoT Device Cybersecurity Requirement Catalog.* (2021). US Department of Commerce. National Institute of Standards and Technology.
13. NISTIR 8228: *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks.* (2019). US Department of Commerce. National Institute of Standards and Technology.

14. NISTIR 8259: *Foundational Cybersecurity Activities for IoT Device Manufacturers.* (2020). US Department of Commerce. National Institute of Standards and Technology.
15. NISTIR 8259A: *IoT Device Cybersecurity Capability Core Baseline.* (2020). US Department of Commerce. National Institute of Standards and Technology.
16. NISTIR 8259B: *IoT Non-technical and Supporting Capability Core Baseline*. (2020). National Institute of Standards and Technology.
17. NISTIR 8259C: *Creating a Profile of the IoT Core Baseline and Non-Technical Baseline.* (2020). National Institute of Standards and Technology.
18. NISTIR 8259D: *Profile using the IoT Core Baseline and Non-Technical Baseline for the Federal Government.* (2020). National Institute of Standards and Technology.
19. *Postmarket Management of Cybersecurity in Medical Devices. Guidance for Industry and Food and Drug Administration Staff*. (2016). Department of Health and Human Services. Food and Drug Administration, 4.
20. NIST Special Publication 800-53r5. *Security and Privacy Controls for Information Systems and Organizations.* (2017). US Department of Commerce. National Institute of Standards and Technology.
21. Fact Sheet: *The FDA's Role in Medical Device Cybersecurity, Dispelling Myths and Understanding Facts.* (2019). Department of Health and Human Services. Food and Drug Administration. Retrieved from: https://www.fda.gov/files/medical%20...fact-sheet.pdf

APPENDIX A: Assessing Enhanced Security

Draft NIST Special Publication 800-172A

Assessing Enhanced Security Requirements for Controlled Unclassified Information

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-172A-draft

NIST published SP.800-172A (above), *Assessing Enhanced Security Requirements for Controlled Unclassified Information* in April 2021.

It is intended for use with SP.800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information.*

SP.800-172A provides procedures for evaluating the ***coverage*** and ***depth*** of a security/risk assessment which, according to its abstract "…can be used to facilitate risk-based decisions by organizations related to the CUI enhanced security requirements."

SP.800-172A uses assessments ***methods*** and ***objects*** along with a set of determination statements related to the CUI security requirement. Methods are ***Examine***, ***Interview*** and ***Test*** with each possessing the attributes *depth* and *coverage*.

Assessments produce *assurance cases* for determining compliance. As defined by NIST "An assurance case is a body of evidence organized into an argument demonstrating that some claim about a system is true". Assurance cases aid in the determination of compliance with the security requirement.

In order to meet the requirements of SP.800-172A a simple matrix has been created in the Security Assessment workbook which contains both method and attribute. This matrix is applied to each enhanced requirement as seen at the far right of figure 1. Each method assigns an attribute-level (***Basic***, ***Focused*** and ***Comprehensive***) for *depth* and *coverage* attributes.

			SP.800-172A		
ENHANCED - SP.800-172	REQUIREMENT		Assessment Method	Depth*	Coverage*
N	0	Verify the integrity of [security-critical or essential software] using root of trust mechanisms or cryptographic signatures.	**Examine**	Comprehensive	Basic
			Interview	Focused	Focused
			Test	Basic	Focused

Figure 1: Enhanced Assessment Requirements (Depth & Coverage)

Applying enhanced security requirement assessment is not required for completion of the Security Assessment nor does it influence satisfaction (i.e., compliance) values (Y/N - 0, 1) or calculation. While not designed for medium-level security assessments its use offers a qualitative view for enhanced security compliance and, as has already been mentioned, can be used to develop assurance cases which aid decision-makers in determining risk and compliance.

The reader is directed to Appendix C of SP.800-172 for complete description and discussion. Note: the assessment process, method and procedure has also been applied to the Security Control Catalog (SP.800-53r5) and can be found in NIST SP.800-53Ar5, *Assessing Security and Privacy Controls in Information Systems and Organizations*, Appendix C.

Finally, assessment methods, definitions and attributes have been reproduced for reference in the Security Assessment workbook.

APPENDIX B: Adversary Effects

Note

Adversary Effects is a new section (Appendix D) included in NIST SP.800-172 (*Enhanced Security Requirements for Protecting Controlled Unclassified Information*).

NIST Special Publication 800-172

Enhanced Security Requirements for Protecting Controlled Unclassified Information

A Supplement to NIST Special Publication 800-171

RON ROSS
VICTORIA PILLITTERI
GARY GUISSANIE
RYAN WAGNER
RICHARD GRAUBART
DEB BODEAU

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-172

Adversary Effects is a new section (Appendix D) included in NIST SP.800-172 (*Enhanced Security Requirements for Protecting Controlled Unclassified Information*). As described:

> *Finally, a protection strategy and adversary effects section describe the potential effects of implementing the enhanced security requirements on risk, specifically by reducing the likelihood of occurrence of threat events, the ability of threat events to cause harm, and the extent of that harm. Five high-level, desired effects on the adversary can be identified:* ***redirect***, ***preclude***, ***impede***, ***limit***, *and* ***expose***.[1]

The effects themselves contain specific classes of effects:

- *Deter*, *divert*, and *deceive* in support of **redirect**
- *Negate*, *preempt*, and *expunge* in support of **preclude**
- *Contain*, *degrade*, *delay*, and *exert* in support of **impede**
- *Shorten* and *reduce* in support of **limit**
- *Detect*, *reveal*, and *scrutinize* in support of **expose**

NIST describes the specific effects as tactical (i.e., pertaining to a specific threat event or scenario). Detailed explanations of each effect can be found in Appendix D.

Using the effect values a matrix has been created as an example of mapping which adverse effects occur if an associated enhanced security control is implemented (Figure 1). There is no effort made to quantify the values either per control or by individual (adversary) effect as none is provided in the NIST publication. A general view, however, of overall impact a particular control has

is achieved by viewing the results in each effect's column. It is clear that controls which are not implemented ('N' or 'D' response) preclude the intended effect whereas 'Y' or 'P' confirm it.

NIST-SP.800-172 Adversary Effects Map

(Ref. Appendix D.)

Adversary Effects							
Control Family	**#**	**C**	**(R)edirect**	**(P)reclude**	**(I)mpede**	**(L)imit**	**(E)xpose**
F1: Access Control	23	N		No	No		
	24	P		Yes	Yes		
	25	Y		Yes	Yes		
F2: Awareness and Training	4	Y			Yes		Yes
	5	N			No		No
F3: Audit and Accountability			No Adverse Effects Listed				
F4: Configuration Management	10	N			No	No	No
	11	P		Yes	Yes		Yes
	12	Y					Yes
F5: Identification and Authentication	12	P		Yes			Yes
	13	P			Yes		
	14	P		Yes			Yes
F6: Incident Response	4	D				No	No
	5	Y		Yes	Yes	Yes	Yes
F7: Maintenance			No Adverse Effects Listed				
F8: Media Protection			No Adverse Effects Listed				
F9: Personnel Security	3	D		No	No		
	4	Y				Yes	
F10: Physical Protection			No Adverse Effects Listed				
F11: Risk Assessment	4	Y		Yes	Yes		Yes
	5	Y		Yes		Yes	Yes
	6		No Adverse Effects Listed				
	7		No Adverse Effects Listed				
	8	Y					Yes
	9	N		No			No
	10	N		No	No		
F12: Security Assessment	5	Y			Yes		Yes
F13: System and Communications Protection	17	Y	Yes	Yes	Yes	Yes	
	18	N		No	No	No	No
	19	N	No	No	No		No
	20	Y		Yes	Yes	Yes	
F14: System and Information Integrity	8	Y		Yes	Yes		Yes
	9	Y					Yes
	10	D		No	No	No	No
	11	P		Yes	Yes	Yes	
	12	P		Yes	Yes	Yes	
	13	Y					Yes
	14	N		No	No		No

There are 34 enhanced-security controls

Figure 1: Adversary Effects Map

Map column definitions:

- **Control Family Name**
- **#** (corresponding Control Family requirement number)
- **C** (compliance value). Compliance is defined as (**Y**)es, (**N**)o, (**P**)artial and (**D**)oes not Apply. Reference Security Assessment *Snapshot* tab for explanation of Compliance value
- **Adversary Effects**: *Redirect*, *Preclude*, *Impede*, *Limit* and *Expose*

If a Control Family contains no adversary effects its listing is highlighted in light **blue**.

Adversary Effects not associated with a particular control requirement are blank.

Positive and negative (or neutral) effects are highlighted in light and medium **gray** respectively.

> **Note**
>
> Unlike other elements of this workbook the values in this mapping table are manually entered.

Adversary Effects have been included in the Security Assessment workbook (to reflect inclusion in SP.800-172) but since they are not ordinal it is not possible to quantify their value. As such, a high-level matrix map has been created to show which effects have been achieved if an enhanced security-control is implemented (Figure 1) with the table providing an overall snapshot of Adversary Effects.

The reader is directed to Appendix D of SP.800-172 for complete description and discussion.

[1] SP.800-172, 8

Index

Glossary

Adversary Effects | the potential effects of implementing the enhanced security requirements on risk, specifically by reducing the likelihood of threat events, the ability of threat events to cause harm, and the extent of that harm.

Availability | Timely, reliable access to data, information, and systems by authorized users.

Best Practices | The set of guidelines, recommendations and industry-standard practices employed to protect information and systems.

CIA | Confidentiality, Integrity and Availability (of Information)

CISA | Cybersecurity and Infrastructure Security Agency (an agency of DHS)

Confidentiality | Assurance that information is not disclosed to unauthorized individuals, processes, or devices.

CUI | Controlled Unclassified Information

Cybersecurity | An approach or series of steps to prevent or manage the risk of damage to, unauthorized use of, exploitation of, and—if needed—to restore electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these systems.

FDA | Food and Drug Administration

FIPS | Federal Information Processing Standard

GAO | Government Accounting Office

HIPAA | Health Insurance Portability and Accountability Act

HITECH | Health Information Technology for Economic and Clinical Health

Impact | The degree of disruption, degradation or damage due to an adverse event

Information Security | The approach to protect and manage the risk to information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Integrity | A property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored.

Internet of Things (IoT) | The interconnection of electronic devices embedded in everyday or specialized objects, enabling them to sense, collect, process, and transmit data. IoT devices include wearable fitness trackers, “smart” appliances, home automation devices, wireless health devices, and cars —among many others.

IT | Information Technology

Likelihood | The probability of an event occurring

MSSP | Managed Security Service Providers

NIST | National Institute of Standards and Technology

NIST Cybersecurity Framework | A widely used, risk-based approach to managing cybersecurity composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Cybersecurity Framework includes references to standards, guidelines, and best practices. The Framework is voluntary for private sector use; federal agencies must use this risk management approach.

OT | Operation Technology

PHI | Protected Health Information. Sometimes called Electronic Protected Health Information (ePHI)

Risk | The extent to which an entity is threatened by a potential circumstance or event. Risk typically is a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks arise from the loss of confidentiality, integrity, or availability of information or information systems. These risks reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Risk Assessment | An analysis and evaluation of the level of risk a threat poses to a system

Risk Management | The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation. Risk management includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

Risk Management | The ability to identify and mitigate risk(s)

SBOM | Software Bill of Materials (used for IoT devices)

Threat | Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability | A weakness in a system, application, or network that is subject to exploitation or misuse.

About the Author

Thomas P. Dover has worked with technology since the early 90's and currently serves as Senior Information Security Specialist for a Health Delivery Organization (HDO) in Pittsburgh, Pennsylvania.

He is a retired Supervisory Special Agent with the US Secret Service and during his tenure with the agency was a founding member of its Electronic Crimes (ECSAP) program; worked on the development of its Critical Systems Protection (CSP) {Threat Assessment} program; and served as Resident Affiliate to the Computer Emergency Response Team (CERT) at Carnegie-Mellon University.

Tom teaches a variety of technology courses at the college level including Cybersecurity, Physical Security, Business Continuity (COOP) and Digital Forensics. He holds a doctorate in Computer Science from Warren University, certification in Computer Security and Information Assurance from George Washington University and several industry-standard (security) certifications.

He can be reached at thomas.dover@bc3.edu.

Detailed Licensing

Overview

Title: Using NIST for Security and Risk Assessment

Webpages: 46

Applicable Restrictions: Noncommercial

All licenses found:

- CC BY-NC 4.0: 76.1% (35 pages)
- Undeclared: 19.6% (9 pages)
- Public Domain: 4.3% (2 pages)

By Page