A Method for Safety of RFID Systems

Tom Karygiannis , Bernard Eydt , Greg Barber, Lynn Bunn, Ted Phillips
National Institute of Standards and Technology, USA

Abstract

The authors, Tom Karygiannis of NIST, and Bernard Eydt, Greg Barber, Lynn Bunn, and Ted Phillips of Booz Allen Hamilton, wish to thank Steven Fick, Rick Korchak, Kate Remley, Jeff Guerrieri, Dylan Williams, Karen Scarfone, and Tim Grance of NIST, and Kenneth Waldrop and Beth Mallory of Booz Allen Hamilton. These individuals reviewed drafts of this document and contributed to its technical content.

The authors would also like to express their thanks to several experts for their critical review and feedback on drafts of the publication. These experts include V.C. Kumar of Texas Instruments; Simson Garfinkel of the Naval Postgraduate School; Peter Sand of the Department of Homeland Security; Erika McCallister of MITRE; and several professionals supporting Automatic Identification Technology (AIT) program offices within the Department of Defense (DoD), especially Nicholas Tsougas, Fred Naigle, Vince Pontani, Jere Engelman, and Kathleen Smith.

During the public comment period we received helpful comments from the following Federal Government agencies: the US Departments of Defense, Health and Human Services, Homeland Security, Labor, and State; the Office of the Director of National Intelligence; the Office of Management and Budget; and the General Services Administration. We also received several helpful contributions from commercial industry, including comments from EPCglobal, VeriSign, and Priway.

Finally, the authors wish to thank the following individuals for their comments and assistance: Brian Tiplady, Daniel Bailey, Paul Dodd, Craig K. Harmon, William MacGregor, Ted Winograd, Russell Lange, Perry F. Wilson, John Pescatore, Ronald Dugger, Stephan Engberg, Morten Borup Harning, Matt Sexton, Brian Cute, Asterios Tsibertzopoulos, Mike Francis, Joshua Slobin, Jack Harris, and Judith Myerson.

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

These guidelines have been prepared for use by Federal agencies. They may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidance made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

2. RFID Technology

This section provides an introduction to RFID technology. It begins with a discussion of the benefits of RFID relative to other automatic identification and data capture (AIDC) technologies. It then reviews the basic components of RFID systems and provides background information needed to understand later material in the document. Readers who already have a strong understanding of RFID technology and applications can skip this section and the discussion in Section 3 about RFID applications.

2.1 RF Subsystem

To enable wireless identification, the RF subsystem consists of two components:

- RFID tags (sometimes referred to as transponders), which are small electronic devices that are affixed to objects or embedded in them. Each tag has a unique identifier and may also have other features such as memory to store additional data, environmental sensors, and security mechanisms.
- RFID readers, which are devices that wirelessly communicate with tags to identify the item connected to each tag and possibly associate the tagged item with related data.

Both the tag and the reader are two-way radios. Each has an antenna and is capable of modulating and demodulating radio signals. Figure 2-1 shows a simple RF subsystem configuration.

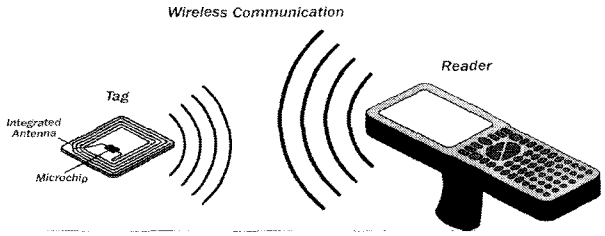

Figure 2-1. An Example of a Simple RF Subsystem

Sections 2.3.1 and 2.3.2 discuss tag and reader characteristics in more detail. Section 2.3.3 explains the fundamentals of tag-reader communication.

2.1.1 Operating Frequencies

The radio frequencies at which a tag transmits and receives signals have implications for:

- **Tag performance characteristics, including operating range, speed of tag reads, and RFID data transfer rate.** In general, as a tag's operating frequency increases, its signals are able to carry more data.6 As a result, higher frequency readers are also able to read more tags in a given period of time. In addition, RFID systems that operate at ultra high frequency (UHF) and microwave frequencies are typically designed to have a longer operating range than LF and high frequency (HF) systems.7 For most applications, the increased speed and operating range are considered advantages. One exception is applications for which security or privacy is a significant concern, such as those that involve financial transactions or personal data. In these cases, the ability of an adversary to read the data more quickly and from a longer distance typically is considered a risk that requires mitigation.
- **The ability of the tag's signal to penetrate materials.** As a general rule, higher frequencies are less able to penetrate substances such as metals or liquids than lower frequencies. Depending on the application, the penetration capabilities of a particular frequency can be either a benefit or a shortcoming. For example, LF communication typically is a requirement when tags are placed inside an animal (or humans, in some emerging medical applications) because RF attenuation in living tissue, which is mostly water, increases significantly as frequency increases. In applications in which security is a significant concern, an organization may want to use a frequency range than can be blocked by a particular material because this enables effective security shielding that might not otherwise be available. Table 2-1 summarizes the ability of RF signals to penetrate various substances.
- **The likelihood of radio interference.** Radio interference is another reason why transmitted signals may not be properly received. Determining the potential sources of radio interference for a particular RFID implementation requires a site survey. RFID systems may experience radio interference from other systems that operate in the same or nearby frequency

band. Interference often is exacerbated when using high power readers or when many readers are collocated. Table 2-2 lists potential sources of interference for RFID systems.

The international portability of tags. The types of systems that use various portions of the electromagnetic spectrum can differ from jurisdiction to jurisdiction because not all regulators assign the same frequencies for the same purposes. If an RFID application requires transporting tags across multiple regulatory jurisdictions, then the system needs to use a frequency range permitted in all of the jurisdictions. Regulations impacting RFID often change, so organizations that use or plan to use RFID technology internationally should monitor relevant developments. Currently, there are frequencies within the LF, HF, and UHF bands that are permitted in most jurisdictions. Also, some tags are frequency-agile, so they can respond to one frequency in one jurisdiction and another in a different jurisdiction.

Table 2-1. Impact of Selected Materials on RF Transmissions9,

Material	LF 30-300 kilohertz (kHz)	HF 3-30 MHz	UHF 300 MHz-1 GHz	Microwave > 1 GHz
	125 or 134 kHz (common US RFID usage)	13.56 MHz[11] (Worldwide ISM band)	433.5-434.5 915 MHz[12] (common US RFID usage)	2.45 GHz[13] (Worldwide ISM band)
Clothing	Transparent	Transparent	Transparent	Transparent
Dry Wood	Transparent	Transparent	Transparent	Absorbent
Graphite	Transparent	Transparent	Opaque	Opaque
Metals	Transparent	Transparent	Opaque	Opaque
Motor Oil	Transparent	Transparent	Transparent	Transparent
Paper Products	Transparent	Transparent	Transparent	Transparent
Plastics	Transparent	Transparent	Transparent	Transparent
Water	Transparent	Transparent	Absorbent	Absorbent
Wet Wood	Transparent	Transparent	Absorbent	Absorbent

Table 2-2. Common Sources of RF Interference

Frequency Range	RFID Applications	Possible Interference Sources in US
Less than 500 kHz	Access control, animal tagging, automobile immobilizers, EAS systems, inventory control, and track and traceability applications	Maritime radio and radio navigation applications
1.95 MHz - 8.2 MHz	EAS systems	Aeronautical radio, amateur, land mobile, maritime mobile radios, and radio location applications
13.553 - 13.567 MHz	Access control, item-level tagging, EAS systems, and smart card applications	ISM applications and private land mobile radio
433.6 - 434.6 MHz	In-transit visibility and supply chain applications	Amateur radio and radio location applications
902 - 928 MHz	Railcar, supply chain, and toll road applications	ISM applications including cordless phones and radio location
2.40 - 2.50 GHz	Real-time location systems (RTLS), and supply chain applications	ISM applications including Bluetooth, cordless phones, and Wi-Fi as well as radio location, and satellite technologies

2.1.1.2 Form Factor

The form factor of a tag refers to its shape, size, packaging, and handling features. To a large extent, a tag's form factor is determined by the characteristics previously discussed, such as power source and functionality. Some important aspects regarding a tag's form factor include the size of the tag, the weight of the tag, and the method by which the tag is affixed to and removed from its associated object. Tags typically vary in size from smaller than a postage stamp to about the size of a common document stapler. Active tags typically are significantly larger and heavier than passive tags because they have an onboard power supply. Tags that integrate environmental sensors are also larger and heavier than those without this functionality. While increasing the computing functionality of a tag increases its cost and power requirements, it may not have an impact on its form factor because the microchip on a passive tag is one of the tag's smallest components. On most passive tags, the largest component on the tag is its antenna.

Tags can be attached to items using an adhesive or can be embedded within the item. The primary concern when a tag is attached to an item is how easily it might be detached, whether accidentally or maliciously. Tags attached to items also are more vulnerable to harsh environmental conditions such as dust, debris, humidity, precipitation, and extreme temperatures. However, the vulnerability is intentional in some cases. For example, RFID tags known as frangible tags allow users to deactivate tags by tearing the tag's antenna from its circuitry. Organizations can create frangible tags on-site using a printer similar to the one shown in Figure 2-2. Tags that are embedded in objects (e.g., smart cards, animal tissue, plastic housing) are less vulnerable to tampering and environmental conditions.

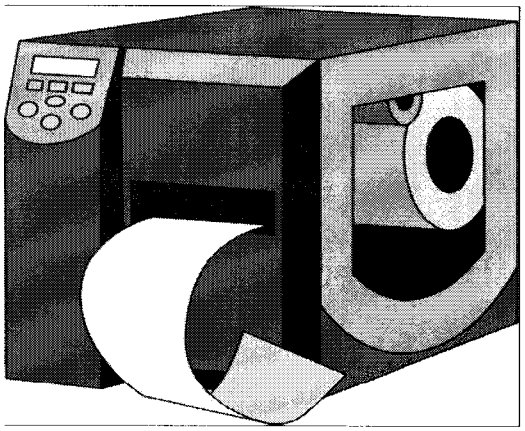

Figure 2-2. RFID Tag Printer

2.1.2 Mobility

A reader's interface with an enterprise subsystem may be wired or wireless. Most wired readers are in fixed locations and support applications in which the tags approach the reader. Some wired readers offer limited mobility using cables. Figure 2-3 shows a reader portal that reads tags on a pallet of boxes moving through the portal. Figure 2-4 shows reader antennas mounted above each toll lane in a series of toll booths. As vehicles pass through one of the toll lanes, the reader reads a transponder that is attached to that vehicle's windshield.

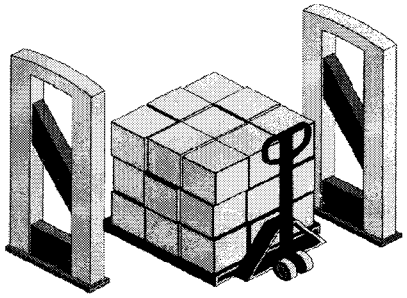

Figure 2-3. Fixed Reader in Item Management Application

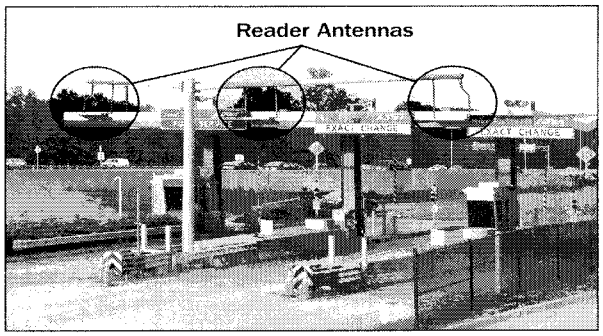

Figure 2-4. Fixed Reader in Automatic Toll Collection Application

In contrast, wireless readers support applications in which personnel must move around to read tags. Figure 2-5 shows an example of a mobile handheld reader. A mobile reader usually uses different communications protocols on its RF and enterprise subsystem interfaces, even though both interfaces are wireless. Institute of Electrical and Electronics Engineers (IEEE) 802.11, also known as Wi-Fi, is a common protocol for the enterprise subsystem interface, although it is also used for the RF interface on some active tag implementations. The most common RF interface protocols are defined in ISO/IEC standards, which include ISO/IEC 14443, ISO/IEC 15693, and the ISO/IEC 18000-series.

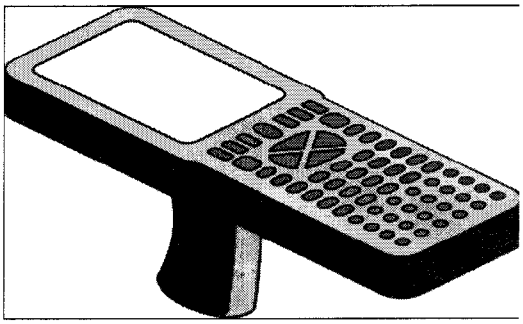

Figure 2-5. Mobile Handheld Reader

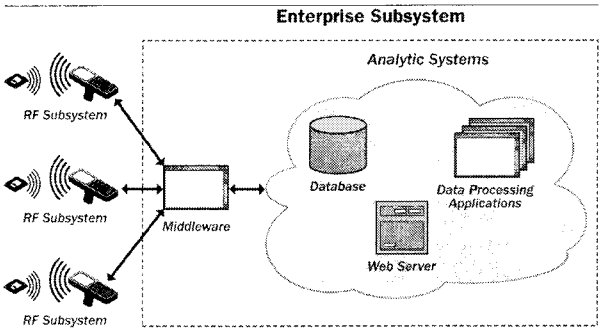

Figure 2-6. RFID System Architecture

3. RFID Applications and Application Requirements

RFID technologies are being deployed by many organizations because they have the potential to improve mission performance and reduce operational costs. To achieve these goals, RFID systems must be engineered to support the specific business processes that the organization is automating. Applications for RFID technologies are diverse because of the wide range of business processes that exist.

RFID security risks and the controls available to mitigate them are also highly varied. Typically, only a subset of the full range of technologies, risks, and controls is applicable to any given RFID implementation. Important business drivers that shape RFID application requirements and the resulting characteristics of RFID systems include:

The general functional objective of the RFID technology (i.e., the application type),

- The nature of the information that the RFID system processes or generates,
- The physical and technical environment at the time RFID transactions occur,
- The physical and technical environment before and after RFID transactions take place, and
- The economics of the business process and RFID system.

This section discusses each of these characteristics in greater detail and provides an overview of common types of RFID applications.

4. RFID Risks

RFID technology enables an organization to significantly change its business processes to:

- Increase its efficiency, which results in lower costs,
- Increase its effectiveness, which improves mission performance and makes the implementing organization more resilient and better able to assign accountability, and
- Respond to customer requirements to use RFID technology to support supply chains and other applications.

The RFID technology itself is complex, combining a number of different computing and communications technologies to achieve the desired objectives. Unfortunately, both change and complexity generate risk. For RFID implementations to be successful, organizations need to effectively manage that risk, which requires an understanding of its sources and its potential characteristics.

This section reviews the major high-level business risks associated with RFID systems so that organizations planning or operating these systems can better identify, characterize, and manage the risk in their environments. The risks are as follows:

- **Business Process Risk.** Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.
- **Business Intelligence Risk.** An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.
- **Privacy Risk.** Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.
- **Externality Risk.** RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people.

An important characteristic of RFID that impacts all of these risks is that RF communication is invisible to operators and users. In other AIDC and IT systems, it often is easier to identify when unauthorized behavior is occurring. This section characterizes the risks listed above in more detail. The security controls that mitigate these risks are discussed in Section 5.

5. RFID Security Controls

This section discusses security controls that can potentially mitigate the business risks associated with RFID systems. As previously discussed, RFID implementations are highly customized. As a result, the security controls listed are not all applicable or

effective for all RFID applications. Organizations need to assess the risks they face and choose an appropriate mix of controls for their environments, taking into account factors such as regulatory requirements, the magnitude of the threat, cost and performance.

Federal agencies should refer to Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems and NIST Special Publication 800-53 (as amended), Recommended Security Controls for Federal Information Systems, when developing or revising policies related to an RFID system. NIST Special Publication 800-100, Information Security Handbook: A Guide for Managers may also be helpful as it provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program.

This section covers security controls applicable to most RFID implementations. It does not address the security of RFID-enabled smart cards and payment systems. This section also does not discuss security controls related to general IT systems, such as network infrastructure, databases, and Web servers because these are already covered by other security requirements and guidelines. For example, EPCIS servers, which can be accessed by trading partners through the Internet, should be protected by the same types of controls that would be used for any other Internet-facing system (e.g., encryption of sensitive communications, access control to prevent unauthorized access to data and systems) to ensure the security of the data collected by the RFID system. Guidelines on topics such as IT server, application, database, and network security are available from many sources, including NIST's Computer Security Resource Center (CSRC).39

RFID security is a rapidly evolving discipline. Although promising research is noted when applicable, this section focuses on controls that are presently commercially available.

5.2 Electromagnetic Shielding

Control: RF shielding encloses an area with a conducting material that limits the propagation of RF signals outside of the shielded area. Shielding can vary in size and form depending on the application.

For example, some RFID-enabled travel documents are protected by a metallic anti-skimming material. This material helps to prevent adversaries from reading the embedded tag when the passport cover is closed. Shipping containers are sometimes shielded to prevent the reading of tags during transit. Shielding is also placed in walls, partitions, or stalls to prevent RF emissions from leaving a confined area. When readers are placed in tunnels on industrial production conveyor belts, the tunnels may be shielded to reduce radio interference. Wrapping a tag in aluminum foil is also an effective means of shielding.

Figure 5-3 shows how shielded partitions can separate collocated readers to prevent interference. The readers near forklift A can operate without inadvertently reading tags on boxes on forklift B due to the shielding in the partition that separates the portals. Shielding may be necessary when middleware is unable to correctly filter duplicate read events from the two portals.

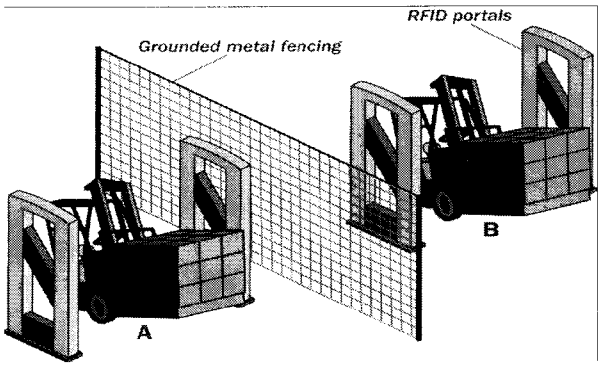

Figure 5-3. Grounded Metal Fencing as Shielding

Applicability: Shielding is applicable for contexts in which eavesdropping or RF radiation is a concern, and the use of temporary shielding would not stop valid transactions.

Benefits: Shielding can limit the ability of eavesdroppers or unauthorized readers to collect data from an RFID system.

Weaknesses:

- Shielding can prevent or hinder legitimate

transactions. For example, shielded containers require objects to be physically removed from the shielding material. This prevents an implementing organization from realizing one of the key benefits of RFID technology, which is to read tags remotely without optical line of sight and additional handling.

It may still be possible for an adversary to place a radio inside the shielded area. The radio could be used for malicious purposes, such as eavesdropping on RFID transactions or causing interference.

6. RFID Privacy Considerations

While this document is primarily about securing RFID systems, privacy issues are often interrelated with security considerations in a manner that one cannot be discussed without the other. For example, protecting privacy often requires technical security controls related to data confidentiality. This section explains what types of information are considered personal, reviews a number of privacy considerations that impact the life cycle of RFID systems, explains general privacy controls, and lists privacy guidance with which US Federal agencies are required to comply.

Privacy regulations and guidance are often complex and change over time. Organizations planning, implementing, or managing an RFID system should always consult with the organization's privacy officer, legal counsel, and chief information officer when developing and enforcing privacy policy related to the system.

7. Recommended Practices

As explained in Sections 2 through 5, there are numerous ways to implement and configure RFID systems to support a wide variety of applications. RFID systems typically must be highly customized to support the business processes they automate; no one-size-fits-all approach will work across implementations. Nevertheless, organizations can benefit from following some general principles when using RFID technology. This section describes a set of recommended security practices that can help organizations manage RFID risks to an acceptable level.

To be most effective, RFID security controls should be incorporated throughout the entire life cycle – from policy development to operations. This section references a five-phase life cycle to help organizations determine the most appropriate actions to take at each point in the development of the RFID system. The life cycle is based on a model introduced in NIST Special Publication 800-64, Security Considerations in the Information System Development Life Cycle.

Organizations may follow a project management methodology or life cycle model that does not directly map to the phases presented here, but the types of tasks and their sequencing are probably similar. The phases of the life cycle are as follows:

Phase 1: Initiation. This phase covers the tasks that an organization should perform before it starts to design its RFID system. These tasks include conducting a risk assessment and developing policy and requirements with which the RFID system must comply.

Phase 2: Acquisition/Development. For the purposes of this guide, the acquisition/development phase is split into two sub-phases:

Phase 2a: Planning and Design. In this phase, RFID network architects specify the standards with which the RFID system must comply, the network infrastructure that will support the system, and the technical characteristics of the RFID system, including the types of tag and readers that will be deployed. This phase should also include site surveys of the facilities and relevant IT infrastructure.

Phase 2b: Procurement. In this phase, the organization specifies the RFID components that must be purchased, the feature sets and protocols they must support, and any standards on which they must be based.

Phase 3: Implementation. In this phase, procured equipment is configured to meet operational and security requirements, RFID data is integrated with legacy enterprise systems, and staff are trained in the proper use and maintenance of the system.

Phase 4: Operations/Maintenance. This phase includes security-related tasks that an organization should perform on an ongoing basis once the RFID system is operational, including conducting periodic security assessments, applying security-related software patches, and reviewing RFID event logs.

Phase 5: Disposition. This phase encompasses tasks that occur when a system or its components have been retired, perhaps as a result of a significant upgrade. These tasks include preserving information to meet legal requirements and disabling or destroying tags and other components when they are taken out of service.

The practices presented in this section are provided in tables corresponding to the life cycle phases. Each practice is accompanied by a brief explanation of the rationale for its inclusion and is rated as "recommended" or "should consider." Organizations are strongly encouraged to adopt the "recommended" practices. Failure to implement them significantly increases the risk of an RFID security failure.

Organizations should also examine each of the "should consider" practices to determine their applicability to the target environment. A "should consider" practice should be rejected only if it is infeasible or if the reduction in risk from its implementation does not justify its cost.

Organizations should develop their RFID security controls based not only on the practices in the tables, but also using other guidelines on security controls. FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, establishes three security categories—low, moderate, and high—based on the potential impact of a security breach involving a particular system. NIST Special Publication 800-53 (as amended), Recommended Security Controls for Federal Information Systems, provides minimum management, operational, and technical security controls for information systems based on the FIPS Publication 199 impact categories. The information in NIST Special Publication 800-53 should be helpful to organizations in identifying controls that are needed to protect networks and systems, which should be used in addition to the specific practices for RFID systems listed in this document. Federal agencies should also use NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, to evaluate their RFID system and select appropriate security controls.

The RFID policies that an organization develops should be consistent with existing IT and operations policies. However, in some cases, the organization may need to modify the existing policies to accommodate the introduction of an RFID system.

Some large organizations may divide RFID-related duties among various teams. For example, one group may be responsible for the RF subsystem, while another might focus on the enterprise subsystem. To assist with this division of labor, the tables in this section identify the affected subsystem or components (e.g., tag or reader) for each of the listed practices.
The tables can also serve as checklists. In particular, the status column on the right is blank so that RFID support staff or auditors can use it to measure progress toward implementation of the practices.

8. Case Studies

This section presents two hypothetical case studies to illustrate how RFID security might be implemented in practice. Although the case studies are fictional, they are intended to resemble real-world activities, including how decision makers address common and expected RFID security problems and their solutions. The case studies do not cover all of the aspects of RFID system engineering or operations that an organization may encounter in its RFID implementation, but rather a representative sample of salient issues. The two case studies are as follows:

Case Study #1: Personnel and asset tracking in a health care environment, and

Case Study #2: Supply chain management of hazardous materials.

In each case study, the fictional organization followed the information system development life cycle introduced in NIST Special Publication 800-64, Security Considerations in the Information System Development Life Cycle, and the practices discussed in Section 7.