United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, House Committee on Homeland Security

For Release on Delivery
Expected at 10:00 a.m. EDT
June 22, 2005

INFORMATION SECURITY

Key Considerations Related to Federal Implementation of Radio Frequency Identification Technology

Statement of Gregory C. Wilshusen, Director
Information Security Issues

June 2005

INFORMATION SECURITY

Key Considerations Related to Federal Implementation of Radio Frequency Identification Technology

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-849T, a report to the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, House Committee on Homeland Security

Why GAO Did This Study

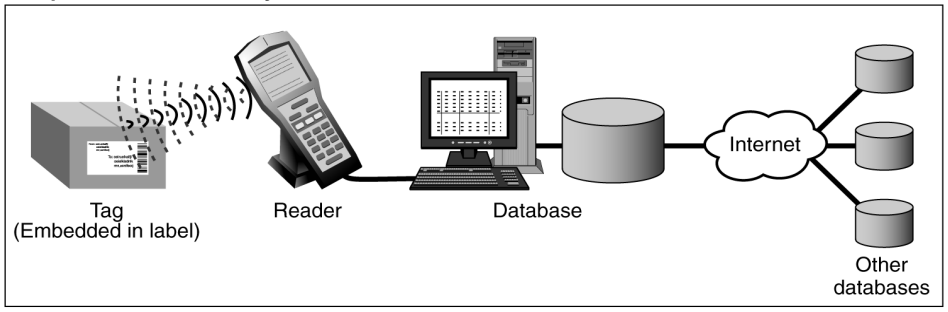
Radio frequency identification (RFID) is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag that is attached to or embedded in an object, such as a product, case, or pallet. Federal agencies have begun implementation of RFID technology, which can offer them new capabilities and efficiencies in operations. For example, the State Department has reported plans to use RFID technology in its electronic passports. The reduced cost of the technology has made the wide-scale use of it a real possibility for government and industry organizations.

As requested, this testimony will provide an overview of the technology and discuss key security, privacy, and other considerations surrounding implementation of the technology in the federal government. It is based on our recently issued report (GAO-05-551).

What GAO Found

The main technology components of an RFID system are a tag, reader, and database. A reader scans the tag for data and sends the information to a database, which stores the data contained on the tag (see figure).

Components of an RFID system



Source: GAO.

The use of tags and databases raises important security considerations related to the confidentiality, integrity, and availability of the data on the tags, in the databases, and in how this information is being protected. Tools and practices such as implementing the risk-based framework mandated by the Federal Information Security Management Act of 2002 and employing encryption and authentication technologies can help mitigate these security considerations.

Key privacy concerns include notifying individuals of the existence or use of the technology; tracking an individual's movements; profiling an individual's habits, tastes, or predilections; and allowing for secondary uses of the information. Tools and practices can help mitigate these considerations, including existing requirements contained in legislation and proposed measures such as a deactivation mechanism on the tag, among others.

In addition to security and privacy, there are other areas of consideration related to the adoption of the technology. These areas include the reliability of the tags and readers; placement and orientation of the tag; costs and benefits associated with implementation; availability of tags; and environmental issues, such as the reuse and recycling of tags.

www.gao.gov/cgi-bin/getrpt?GAO-05-849T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Greg Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to present a summary of our work in the area of radio frequency identification (RFID) technology.[1] RFID is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag. The tag can be attached to or embedded in the object to be identified, such as a product, case, or pallet. RFID provides identification and tracking capabilities by using wireless communication to transmit data.

The technology can provide a more efficient method for federal agencies, manufacturers, retailers, and suppliers to collect, manage, disseminate, store, and analyze information on inventory, business processes, and security controls, among other functions, by providing real-time access to information. Several federal agencies have already begun testing and using the technology. For example, the State Department has reported plans to use RFID technology in its electronic passports.

As requested, in my testimony today, I will present an overview of RFID technology and discuss the security, privacy, and other considerations surrounding RFID technology implementation in the federal government.

My testimony today is based on our recently published report[2] on RFID technology and was prepared in accordance with generally accepted government auditing standards.

Results in Brief

RFID is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag. The main technology components of an RFID system are a tag, reader, and database. A radio frequency reader scans the tag for data and sends the information to a database, which stores the data contained on the tag. Passive tags do not contain their own power source, such as a battery. The development of these inexpensive tags has created a revolution in RFID adoption and made wide-scale use of them a real possibility for government.

[1]GAO, *Information Security: Radio Frequency Identification Technology in the Federal Government*, GAO-05-551 (Washington, D.C.: May 27, 2005.)

[2]GAO-05-551.

Several security and privacy issues are associated with federal and commercial use of RFID technology. The security of tags and databases raises important considerations related to the confidentiality, integrity, and availability of the data on the tags, in the databases, and in how this information is being protected. Tools and practices to address these security issues, such as compliance with the risk-based framework mandated by the Federal Information Security Management Act (FISMA) of 2002[3] and employing encryption and authentication technologies, can help agencies achieve a stronger security posture. Among the key privacy issues are notifying individuals of the existence or use of the technology; tracking an individual's movements; profiling an individual's habits, tastes, or predilections; and allowing secondary uses of information. The Privacy Act of 1974 limits federal agencies' use and disclosure of personal information,[4] and the privacy impact assessments required by the E-Government Act of 2002 provide an existing framework for agencies to follow in assessing the impact on privacy when implementing RFID technology.[5] Additional measures proposed to mitigate privacy issues, such as using a deactivation mechanism on the tag, incorporating blocking technology to disrupt transmission, and implementing an opt-in/opt-out framework for consumers are in progress.

In addition to security and privacy, there are other areas to consider related to the adoption of the technology. These areas include the reliability of the tags and readers, which do not consistently work with some products or in certain situations; placement and orientation of the tag, which can contribute to how effectively a tag can be read; costs and benefits associated with implementation; availability of tags; and environmental issues related to the reuse and recycling of tags.

Background

RFID technology uses wireless communication in radio frequency bands to transmit data from tags to readers. A tag can be attached to or embedded in an object to be identified, such as a product, case, or pallet. A reader scans the tag for data and sends the information to a database, which stores the data contained on the tag. For example, tags can be

[3]44 U.S.C. § 3544 (b).

[4]5 U.S.C. § 552 a(a)(4).

[5]44 U.S.C. § 3501 note. See Office of Management and Budget M-03-22, Sept. 26, 2003.

placed on car windshields so that toll systems can quickly identify and collect toll payments on roadways.

Interest in RFID technology began during World War II and has increased in the past few years. During the war, radio waves were used to determine whether approaching planes belonged to allies or enemies. Since then, exploration in radio technology research and development in commercial activities continued through the 1960s and evolved into marked advancements in the 1970s by companies, academic institutions, and the U.S. government. For example, at the request of the Department of Energy, Los Alamos National Laboratory developed a system to track nuclear materials by placing a tag in a truck and readers at the gates of secure facilities. This is the system used today in automated toll payment systems.

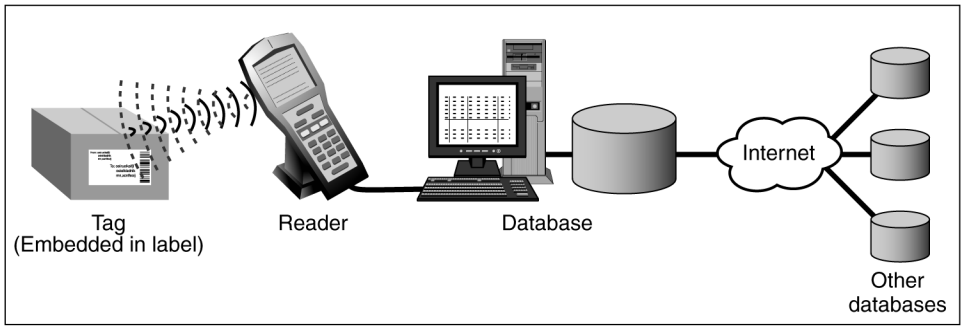
The technology offers several improvements over its predecessor technologies, such as barcodes and magnetic stripe cards. For instance, a tag can carry more data than a barcode or magnetic stripe and can be reprogrammed with new information if necessary. Additionally, tags do not typically require a line of sight to be read, as barcodes do, and can be read more rapidly and over greater distances. Mandates by large retailers and the Department of Defense (DOD) requiring their top suppliers to use RFID tags, along with technological advancements and decreased costs, have spurred the proliferation of this technology. RFID technology is now being used in a variety of public and private-sector settings, ranging from tracking books in libraries to authenticating a key in order to start a vehicle.

RFID Technology Overview

RFID is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag. A radio frequency reader scans the tag for data and sends the information to a database, which stores the data contained on the tag.

The main technology components of an RFID system are the tag, reader, and database. (See fig. 1.)

Figure 1. Main Components of an RFID System



Source: GAO.

The Tag

An RFID tag, or transponder, consists of a chip and an antenna . A chip can store a unique serial number or other information based on the tag's type of memory, which can be read-only, read-write, or write-once read-many. The antenna, which is attached to the microchip, transmits information from the chip to the reader. Typically, a larger antenna indicates a longer read range. The tag is attached to or embedded in an object to be identified, such as a product, case, or pallet, and can be scanned by mobile or stationary readers using radio waves.

The simplest version of a tag is a passive tag. **Passive tags** do not contain their own power source, such as a battery, nor can they initiate communication with a reader. Instead, the tag responds to the reader's radio frequency[6] emissions and derives its power from the energy waves transmitted by the reader. Under perfect conditions, the tags can be read[7] from a range of about 10 to 20 feet.[8] The cost of passive tags ranges from 20 cents to several dollars. Costs vary based on the radio frequency used, amount of memory, design of the antenna, and packaging around the transponder, among other tag requirements. Passive tags can operate at various frequencies. Examples of passive tag applications include mass transit passes, building access badges, and consumer products in the

[6]Frequency is the number of radio waves that pass a given point during a fixed period of time (e.g., the number of complete oscillations per second of energy).

[7]The read range of a tag is based on the size of the antenna, frequency used, power of the reader, and the material between the tag and the reader.

[8]Although these tags can theoretically be read at 30 feet, when factoring in circumstances that can interfere with the read range (e.g., water and metal), the actual read distance is reduced to 10 feet or less.

supply chain. The development of these inexpensive tags has created a revolution in RFID adoption and made wide-scale use of them a real possibility for government and industry organizations.

Semipassive tags[9] also do not initiate communication with the reader but contain batteries that allow the tag to perform other functions, such as monitoring environmental conditions and powering the tag's internal electronics. These tags do not actively transmit a signal to the reader. Some semipassive tags remain dormant (which conserves battery life) until they receive a signal from the reader. The battery is also used to facilitate information storage. Semipassive tags can be connected to sensors to store information for container security devices.

Active tags contain a power source and a transmitter, in addition to the antenna and chip, and send a continuous signal. These tags typically have read/write capabilities—tag data can be rewritten and/or modified. Active tags can initiate communication and communicate over longer distances—up to 750 feet, depending on the battery power. The relative expense of these tags makes them an option for use only where their high cost can be justified. Active tags are more expensive than passive, costing about $20 or more per tag. Examples of active tag applications are toll passes, such as "E-Z pass," and the in-transit visibility applications on major items and consolidated cargo moved by DOD.

Tags have various types of memory, including read-only, read-write, and write-once read-many. Read-only tags have minimal storage capacity (typically less than 64 bits) and contain permanently programmed data that cannot be altered. These tags primarily contain item identification information and have been used in libraries and video rental stores. Passive tags are typically read-only. In addition to storing data, read-write tags can allow the data to be updated when necessary. Consequently, they have larger memory capacity and are more expensive than read-only tags. These tags are typically used where data may need to be altered throughout a product's life cycle, such as in manufacturing or in supply chain management. A write-once, read-many tag allows information to be stored once, but does not allow subsequent alterations to the data. This tag provides the security features of a read-only tag while adding the additional functionality of read/write tags.

[9]Semipassive tags are also referred to as semiactive or battery-assisted passive tags.

The Reader

In order for an RFID system to function, it needs a reader, or scanning device, that is capable of reliably reading the tags and communicating the results to a database. A reader uses its own antenna to communicate with the tag. When a reader broadcasts radio waves, all tags designated to respond to that frequency and within range will respond. A reader also has the capability to communicate with the tag without a direct line of sight, depending on the radio frequency and the type of tag (active, passive, or semipassive) used.

Readers can process multiple items at once, allowing for increased read processing times. They can be mobile, such as handheld devices that scan objects like pallets and cases, or stationary, such as point-of-sale devices used in supermarkets. Readers are differentiated by their storage capacity, processing capability, and the frequencies they can read.

The Database

The database is a back-end logistic information system that tracks and contains information about the tagged item. Information stored in the database can include item identifier, description, manufacturer, movement of the item, and location. The type of information housed in the database will vary by application. For instance, the data stored for a toll payment system will be different than the data stored for a supply chain. Databases can also be linked into other networks, such as the local area network, which can connect the database to the Internet. This connectivity can allow for data sharing beyond the local database from which the information was originally collected.

RFID Systems Operate on Radio Frequencies

Choice of radio frequency is a key operating characteristic of RFID systems. The frequency largely determines the speed of communication and the distance from which the tag can be read. Generally, higher frequencies indicate a longer read range. Certain applications are more suitable for one type of frequency than other types, because radio waves behave differently at each of the frequencies. For instance, low-frequency waves can penetrate walls better than higher frequencies, but higher frequencies have faster data rates. RFID systems use an unlicensed frequency range, classified as industrial-scientific-medical or short-range devices, which is authorized by the Federal Communications Commission (FCC).[10] Devices operating in this unlicensed bandwidth may not cause

[10]In the United States, the FCC authorizes the use of the 2.4 GHz and the 902-928 MHz frequency range for industrial-scientific-medical and short-range devices, which includes RFID technology.

harmful interference and must accept any interference received. The FCC also regulates the specific power limit associated with each frequency. The combination of frequency and allowable power levels determine the functional range of a particular application, such as the power output of readers.

The U.S. Department of State has reported plans to use RFID technology in its electronic passports.[11] The United States and other countries are anticipating using the International Civil Aviation Organization[12] (ICAO) Document 9303 standard, which prescribes an international format for passports, visas, and other official machine-readable travel documents.

Security and Privacy Considerations with RFID

The security of tags and databases raises important considerations concerning the confidentiality, integrity, and availability of the data on the tags, in the databases, and in how this information is being protected. Measures to address these security issues, such as compliance with the risk-based framework mandated by the Federal Information Security Management Act (FISMA) of 2002 and employing encryption and authentication technologies, can help achieve a stronger security posture. Among the key privacy issues are notifying individuals of the existence or use of the technology; tracking an individual's movements; profiling an individual's habits, tastes or predilections; and allowing for secondary uses of information. Measures to mitigate these issues are in progress.

Security Considerations Relate to Data Confidentiality, Integrity, and Availability

Several agencies identified data confidentiality, integrity, and availability as key security considerations with implementing RFID technology. Specifically, these issues included ensuring that only authorized readers or personnel have access to information, maintaining the integrity of the data on the chip and stored in the databases, and ensuring that critical data is fully available when necessary. Other issues with implementing the technology included the potential for various attacks, such as

[11]The proposed U.S. electronic passport will resemble a regular passport with the addition of a small RFID chip embedded in the back cover. The chip will securely store the same data visually displayed on the photo page of the passport and will also include a digital photograph.

[12]ICAO was chartered by the United Nations to regulate international aviation and includes the United States and 188 other nations.

counterfeiting or cloning,[13] replay,[14] and eavesdropping; the possibility of electronic collisions when multiple tags and/or readers are present; and the presence of unauthorized components that may interfere or imitate legitimate system components.

Without effective security controls, data on the tag can be read by any compliant reader; data transmitted through the air can be intercepted and read by unauthorized devices; and data stored in the databases can be accessed by unauthorized users.

Practices and Tools in Place to Address Security Considerations

Using security practices and tools such as the risk-based framework mandated by FISMA, encryption, and authentication can help mitigate the security considerations associated with implementing RFID technology.

Implementing the security practices required in FISMA can help strengthen the security of RFID systems that store information transmitted from tags. FISMA requires each agency, including agencies with national security systems, to develop, document, and implement an agencywide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Specifically, this program is to include

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;

[13]Cloning an RFID tag occurs when an attacker produces an unauthorized copy of a legitimate tag.

[14]A replay attack is an attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it.

- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;

- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk but no less than annually, and which includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;

- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

- procedures for detecting, reporting, and responding to security incidents; and

- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Encrypting the data on the tags, in the air, or stored in a database may also reduce the risk of unauthorized use or changes. Using encryption may be particularly relevant for applications where sensitive information is contained on the tag. Encryption is the process of transforming ordinary data (commonly referred to as plaintext) into code form (ciphertext) using a special value known as a key and a mathematical process called an algorithm. Cryptographic algorithms are designed to produce ciphertext that is unintelligible to unauthorized users. Decryption of ciphertext is possible by using the proper key. Encryption technologies can be used to (1) hide information content, (2) prevent undetected modification, and (3) prevent unauthorized use. When properly implemented, encryption technologies may provide assurance regarding the confidentiality, integrity, or origin of information that has been exchanged. It may also provide a method by which the authenticity can be confirmed. Without strong encryption, the data may not be kept confidential.

Authentication, which is the process of verifying the claimed identity of a user, can be used between tag and reader as a way to mitigate security risks. Authentication of readers can help prevent the unauthorized reading and/or writing to tags.

Privacy Issues Surrounding RFID Use

The extent and nature of the privacy issues related to the federal and commercial use depends on the specific proposed use. For example, using the technology for generic inventory control would not likely generate substantial privacy concerns. However, the use of RFIDs by the federal government to track the movement of individuals traveling within the United States could generate concern by the affected parties. Privacy issues associated with RFID implementation include notifying individuals of the existence or use of the technology; tracking an individual's movements; profiling an individual's habits, tastes or predilections; and allowing for secondary uses of information.

- **Notification.** Individuals may not be aware that the technology is being used unless they are informed that the devices are in use. Therefore, unless they are notified, consumers may not be aware that the RFID tags are attached to or embedded in items they are browsing or purchasing or that the items purchased are being scanned.

- **Tracking.** Tracking is real-time, or near-real-time, surveillance in which a person's movements are followed through RFID scanning. Media reports have described concerns about ways in which anonymity is likely to be undermined by surveillance. As previously reported, many civil liberties groups are concerned about the application of this technology to track individuals' movements, such as in a public school setting, and the resulting loss of anonymity in public places.[15] Additionally, periodic public surveys have revealed a distinct unease with the potential ability of the federal government to monitor individuals' movements and transactions.

- **Profiling.** Profiling is the reconstruction of a person's movements or transactions over a specific period of time, usually to ascertain something about the individual's habits, tastes, or predilections. Because tags can contain unique identifiers, once a tagged item is associated with a particular individual, personally identifiable information can be obtained and then aggregated to develop a profile of the individual. As previously reported,[16] profiling for race, ethnicity, or national origin has caused public debate in recent years. Both tracking and profiling can compromise an individual's privacy and anonymity.

[15]GAO, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

[16]GAO-03-174.

- **Secondary uses.** In addition to issues about the planned uses of such information, there is also concern surrounding the possibility that organizations could develop secondary uses for the information; that is, information collected for one purpose tends over time to be used for other purposes as well. This has been referred to as "mission-" or "function-creep." The history of the Social Security number, for example, gives ample evidence of how an identifier developed for one specific use has become a mainstay of identification for many other purposes, governmental and nongovernmental.[17] Secondary uses of the Social Security number have been a matter not of technical controls but rather of changing policy and administrative priorities.

  The widespread adoption of the technology can contribute to the increased occurrence of these privacy issues. As previously mentioned, tags can be read by any compatible reader. If readers and tags become ubiquitous, tagged items carried by an individual can be scanned unbeknownst to that individual. Further, the increased presence of readers can provide more opportunities for data to be collected and aggregated. As the uses of technology proliferate, consumers have raised concerns about whether certain collected data might reveal personal information such as medical predispositions or personal health histories and that the use of this information could result in denial of insurance coverage or employment to the individual. For example, the use of RFID technology to track over-the-counter or prescription medicines has generated substantial controversy.

Practices and Tools to Mitigate Privacy Issues Are in Progress

Implementing privacy practices and tools, such as existing requirements contained in the Privacy Act of 1974 and the E-Government Act of 2002, and employing proposed measures such as a deactivation mechanism on the tag, blocking technology to disrupt transmission, and an opt-in/opt-out framework for consumers can help mitigate some of these privacy issues. These proposed techniques may address some of the privacy issues and are in progress.

An existing legal framework that addresses the privacy issues under which federal agencies operate when implementing any new information technology is defined in the Privacy Act of 1974, which limits federal agencies' use and disclosure of personal information. The act's protections

[17]GAO, *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352 (Washington, D.C.: May 31, 2002).

are keyed to the retrieval of personal information by a "name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."[18] The Privacy Act generally covers federal agency use of personal information, regardless of the technology used to gather it. As a practical matter, however, the Privacy Act is likely to have a limited application to the implementation of RFID technology because the act only applies to the information once it is collected, not to whether or how to collect it. The E-Government Act's privacy impact assessments requirement, however, provides a means of evaluating whether or not to collect information based on privacy concerns.

Employing a mechanism that can deactivate, or "kill," a tag at the point of sale, can prevent tracking of the individual and item once the tag leaves a store. This feature would still provide the supply chain tracking benefits to the retailer without providing additional information about the consumer beyond the point of sale. However, enforcement may be a challenge, as a tag may inadvertently be deactivated or remain dormant with the potential to be reactivated. Additionally, consumers opting to have the tags deactivated may have to undergo additional procedures that may cost time or money.

Another proposed method is blocking technology. Devices that can disrupt the transmission of all or selected information contained on a tag would be embedded in an object that is carried or worn near RFID tags that the individual wants blocked. This technology, however, has not yet been fully developed. One challenge to its development may be the constant proximity required between the blocker tag and the tag in order to disrupt data transmission. Consumers may not consistently remember to juxtapose the tags, thereby reducing the effectiveness of the technology. A physical method of blocking currently in use is aluminum-coated Mylar[19] bags, which can absorb or diffuse RFID signals when placed over the tag. An example is in toll payment systems where aluminum-coated Mylar bags are issued along with the tag so that drivers can place their tags in the bag to prevent them from being read inadvertently. Additionally, the State Department is reported to have plans to include metal inside U.S. passport

[18]5 U.S.C. §552a(a)(4).

[19]Mylar is a registered trademark of Dupont Tejin Films that generally refers to plastic film. A common application is packaging film for food, electronics, and medical devices.

jackets to help prevent the chip from being read by anyone except customs and border agents.

Government and industry groups have also proposed using an opt-in/opt-out framework. This framework would provide consumers with an option to voluntarily participate in RFID transactions that gather data about them. Consumers would be informed of the existence of the tags and the type of information that would be collected and could then decide whether to participate in the transaction or opt out. A concern of this hybrid system is the potential disparity in benefits received between consumers who opt in versus those who opt out, similar to customer loyalty cards, and the notion that this framework might penalize consumers who articulate their privacy preferences. Also, a study by the RAND Corporation has suggested that organizations using RFID workplace access devices should implement "fair information practices" and communicate those policies to employees.[20]

Other Areas of Consideration Are Relevant to RFID Adoption

In addition to privacy and security, other areas of consideration related to the adoption of RFID technology include the reliability of tags and readers, the placement of the tags, the costs and benefits of implementation, the availability of tags, and environmental issues.

Reliability. Currently, tags are not always reliable and will not work with some products or in certain situations. When something close to the reader or tag interferes with the radio waves, read-rate accuracy decreases. For instance, defective tags created by the manufacturer can be unreadable or tags may be damaged during the supply chain process. Additionally, readers can produce false negatives (a reader does not read a valid tag that passes within the prescribed range) or false positives (a tag not intended to be read inadvertently passes within range of a reader), which typically occur with closely packed items where multiple tags are near each other. Further, environmental conditions, such as temperature and humidity, can make tags unreadable. Experts have indicated that tags read at high speeds have a significant decrease in read rate. As the technology continues to mature, these limitations may eventually be addressed, but currently they remain a challenge to organizations.

[20]The RAND Corporation, *Privacy in the Workplace: Case Studies on the Use of Radio Frequency Identification in Access Cards*, RB-9107-RC (Santa Monica, Calif.: 2005).

Placement. The placement and orientation of the tag contributes to how effectively the reader can scan it. Factors to consider in tag placement are read and nonread points on objects such as items, cases, or pallets; locations that minimize the risk of damage to the tag and have the highest potential for a successful passive tag reading; and read points in specific environments, such as an item running through a conveyor belt at various speeds.

Some organizations, such as DOD, have documented procedures for tag placement to help ensure placement precision, consistency, and efficiency. Determining optimal tag placement may require software or an automated application to improve this otherwise manual process.

Costs and Benefits. Best practices for information technology investment dictate that prior to making any significant project investment the costs and benefits of the system should be analyzed and assessed in detail.[21] The cost of the tags generally falls on the supplier, as it is the supplier who tags the items. Retailers see benefits from RFID tags such as improved product visibility during the supply chain process. Suppliers can also see such benefits when they go beyond the "slap and ship"[22] model and find new ways to make the technology add value to gain a return on investment. According to the National Institute of Standards and Technology, smaller suppliers may earn little to no return because the costs associated with implementing the technology, such as hardware, software, infrastructure middleware,[23] and training will be a substantial portion of a small supplier's budget. Additionally, their price per-tag may be high since they do not order large quantities. Organizations need to determine if the cost of implementing this technology, which is still in the early stages of adoption, is worth the increased ability to collect and analyze data.

Availability. With increasing adoption of RFID technology, the availability of tags may emerge as a growing concern. The increased adoption of the technology will result in greater demand for tags. As a

[21]GAO, *Aviation Security: Challenges in Using Biometric Technologies*, GAO-04-785T (Washington, D.C.: May 19, 2004).

[22]Slap and ship" is when a supplier tags the products with an RFID tag right before shipping them to the retailer. Suppliers who slap and ship generally will not benefit from the technology because they do not make use of it for their own benefit.

[23]Middleware is software that connects two otherwise separate applications.

result, the demand for tags may eventually outstrip the supply. Even if industry can keep up with the demand, damage to the tags during production may create a shortage. For instance, according to a research group's survey of RFID vendors, up to 30 percent of chips are damaged during production when they are attached to their antennae, and an additional 10 to 15 percent are damaged during the printing process. Improving tag manufacturing and quality control processes may help increase the availability of operative tags.

Environment. In September 2004, the Environmental Protection Agency (EPA) and the Office of the Federal Environmental Executive (OFEE) cohosted a workshop on the impact of tags on the reuse and recycling of packaging materials. Tags contain silicon, adhesives, and nickel, and the antennae are typically made from copper, aluminum, or, if printed, silver. According to OFEE, these elements of the tags are potential contaminants for recyclers and manufacturers using recycled materials. As such, OFEE and EPA believe that it is essential that these industries begin to understand the potential impacts of having tags on packaging materials and pallets and plan how to minimize the impact on the environment. One manufacturer remarked on the lack of practicality in recycling because of the small amount of silicon used in the chip. Currently, EPA does not provide clear national guidelines on electronic waste (e-waste) disposal nor has it defined its e-waste goals and measures. Consequently, states are pursuing their own mechanisms to regulate e-waste. As tagging begins to include cases, additional environmental issues may arise because cases are not reusable, in contrast to the pallets, which are reusable.

In summary, RFID technology can provide new capabilities as well as an efficient method for federal agencies, manufacturers, retailers, and other organizations to collect, manage, disseminate, store, and analyze information on inventory, business processes, and security controls by providing real-time access to information. The use of the technology, however, raises several security and privacy considerations that may affect federal agencies' decisions to implement the technology. Key security issues include protecting the confidentiality, integrity, and availability of the data and information system. The privacy issues include notifying consumers; tracking an individual's movements; profiling an individual's habits, tastes, and predilections; and allowing for secondary uses of information. In addition, other areas such as the reliability, placement, and availability of tags, along with the cost and benefits of implementation and environmental concerns, are factors to consider.

Mr. Chairman, this concludes my statement. I look forward to your questions.

Contacts and Acknowledgments

Should you have any questions about this testimony, please contact Greg Wilshusen at (202) 512-6244 or by e-mail at wilshuseng@gao.gov. Other individuals who made key contributions to this testimony include Nancy Glover, Min Hyun, Stephanie Lee, and Suzanne Lightman.

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER