

Department of Homeland Security REAL ID Security Plan Guidance Handbook

Version 1.0 — February 2009



For U.S. State and Territory Department of Motor Vehicle Office Use Only

REAL ID Security Plan Guidance Handbook

Executive Summary

This REAL ID Security Plan Guidance Handbook provides security plan guidance and recommendations for States seeking to implement REAL ID. The Handbook provides guidance on topics such as how to secure facilities involved in the enrollment, production, and issuance of REAL ID driver's licenses and identification cards, card design and security, privacy, personnel security, and the contents of the security plan that States should submit as part of their REAL ID full compliance certification packages.²

² This document will henceforth use the term "States" to refer to the 56 jurisdictions covered by the REAL ID Act of 2005. This number includes the 50 States, the District of Columbia, and five territories of the United States.

For U.S. State and Territory Department of Motor Vehicle Office Use Only

REAL ID Security Plan Guidance Handbook

TABLE OF CONTENTS

1	Introduction	1-1
1.1	Purpose	1-1
1.2	Scope.....	1-2
1.3	Intended Audience	1-2
1.4	References.....	1-2
2	Security Matrix.....	2-1
2.1	Theft of sensitive components.....	2-1
2.2	Theft of manufacturing or production equipment	2-2
2.3	Unauthorized access to Personally Identifiable Information	2-3
3	Best Practices	3-1
3.1	Physical Security	3-1
3.1.1	Facility Access	3-1
3.1.2	Storage of Sensitive Components.....	3-6
3.1.3	Security of Production Equipment.....	3-7
3.1.4	Contractor Facilities	3-8
3.2	Access Control	3-8
3.2.1	Employee Badges and Credentials.....	3-8
3.2.2	Guards	3-9
3.2.3	Control by Staff	3-9
3.2.4	Automated Systems	3-9
3.2.5	Controlled Access to Terminals and Data Storage.....	3-9
3.2.6	Visitor Control	3-10
3.3	Security of Personally Identifiable Information.....	3-10
3.3.1	Information Technology Systems and Data Storage Security	3-10
3.3.2	Laptops and Portable Storage Media	3-10
3.3.3	Destruction of Media Containing Personally Identifiable Information	3-10
3.3.4	Privacy Policy and the Fair Information Practice Principles	3-11

For U.S. State and Territory Department of Motor Vehicle Office Use Only

REAL ID Security Plan Guidance Handbook

3.3.5	Privacy Impact Assessment.....	3-11
3.4	REAL ID DL/ID Design and Security	3-12
3.4.1	Choosing Security Features.....	3-12
3.4.2	Serialized Card Bodies.....	3-13
3.4.3	Handling of Sensitive Components.....	3-13
3.4.4	Monitoring Document Security and Integrity.....	3-14
3.4.5	Markings for Compliant DL/IDs.....	3-14
3.4.6	Marking Temporary or Limited-Term REAL ID DL/IDs	3-15
3.4.7	Marking of Non-Compliant DL/IDs.....	3-15
3.4.8	Encryption of the 2D Barcode.....	3-16
3.5	Personnel Security.....	3-16
3.5.1	Background Checks	3-16
3.5.2	Training	3-18
3.6	Emergency/Incident Response	3-19
3.7	Audit Controls	3-19
4	Security Plan	4-1
4.1	Plan Contents	4-1
4.1.1	Physical Security and Access Control Methods (Handle as Sensitive Security Information).....	4-1
4.1.2	Security of Personally Identifiable Information.....	4-3
4.1.3	Card Security Features (Handle as Sensitive Security Information)	4-4
4.1.4	Biometrics Usage	4-4
4.1.5	Personnel Security	4-4
4.1.6	Training	4-4
4.1.7	Emergency/Incident Response Plans.....	4-5
4.1.8	Internal Audit Controls (Handle as Sensitive Security Information).....	4-5
5	Handling of Sensitive Security Information.....	5-1
5.1	Information Designated as Sensitive Security Information	5-1
5.2	Access to Sensitive Security Information	5-1
5.3	Protection of Sensitive Security Information	5-1

For U.S. State and Territory Department of Motor Vehicle Office Use Only

REAL ID Security Plan Guidance Handbook

5.4	Storage	5-2
5.5	Marking Documents SSI	5-2
5.6	Destruction	5-2
6	APPENDIX A: Acronyms	6-1
7	APPENDIX B: Terms and Definitions	7-1
8	APPENDIX C: SSI Training Guidance	8-1
9	APPENDIX D: SSI Guidance Brochure	9-1

1 INTRODUCTION

1.1 *Purpose*

The REAL ID regulation requires that States submit to the Department of Homeland Security (DHS), for REAL ID full compliance certification, a REAL ID security plan. The security plan which the State prepares and submits as part of its certification package will be reviewed by DHS in making the determination that the State complies with the requirements of the REAL ID regulation.

This REAL ID Security Plan Guidance Handbook provides States' Department of Motor Vehicle (DMV) agencies with information, guidance and recommended best practices that can be used to meet the REAL ID regulation security plan requirements. The requirements for a REAL ID security plan are located in Subpart D, §37.41 of the REAL ID regulation. At a minimum, the plan's content should address:

- The physical security of facilities used to produce or store materials used for REAL ID driver's licenses and identification cards (DL/IDs),
- The security of personally identifiable information (PII) maintained at DMV locations,
- The physical security features on the cards,
- Access control for facilities and systems,
- Fraudulent document recognition and security awareness training,
- Emergency/incident response,
- Internal audit controls, and
- An affirmation that it has the authority to produce, revise, expunge and protect the confidentiality of REAL ID DL/IDs for programs that require special licensing or identification.

Section 2 of this document provides a matrix identifying possible threats to the security of REAL ID DL/IDs and the sections of this document that discuss how best to approach and remedy those threats.

Section 3 of this document provides best practice recommendations to address several potential REAL ID DL/ID security threats. Section 3 includes guidance on physical security, access control, the security of PII, REAL ID DL/ID design and security, personnel security, emergency/incident response and audit controls.

Section 4 of this document provides a check list that explains the contents of the plan as listed in §37.41 of the REAL ID regulation. The State's plan should address each of these questions in this section to ensure that all items are adequately covered by the plan.

Section 5 of the document provides guidance on handling the Sensitive Security Information (SSI) generated and used in the REAL ID security planning process.

1.2 *Scope*

The REAL ID regulation requires that “each State submit a single security plan to address DMV facilities involved in the enrollment, issuance, manufacturing and production of drivers’ licenses and identification card.”³ This may include the:

- Enrollment of individual applicants in facilities that handle and store PII.
- Issuance of personalized cards to individuals via mail, in person over-the-counter (OTC), or other means.
- Manufacturing of the materials used to produce cards. This includes substrates, card blanks, laminates, security devices, and other physical components of the cards.
- Production or personalization of individualized DL/IDs in central issuance, over-the-counter, or hybrid facilities.

The term “facilities” will be used hereafter to cover any facility where REAL ID DL/IDs are manufactured, produced, issued or where applicants are enrolled. With the exception of section 3.4.7 of this document which addresses the marking of cards produced in accordance with §37.71 of the REAL ID regulation, the guidance provided in this document applies only to REAL ID DL/IDs. However, a State may apply this guidance to its entire DL/ID production if it chooses to do so.

1.3 *Intended Audience*

The intended audience for this document is a State that is seeking to meet the requirements of the REAL ID regulation.

1.4 *References*

1. “Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Final Rule,” 73 FR 5272 (Jan. 29, 2008), codified at 6 Code of Federal Regulations (CFR) Part 37. You can find a copy of the regulation at www.dhs.gov/realid.
2. The REAL ID Act of 2005, Public Law 109-13, 119 Stat. 231, 302 (May 11, 2005) (codified at 49 U.S.C. 30301 note).
3. American Association of Motor Vehicle Administrators (AAMVA) Personal Identification – AAMVA International Specification - DL/ID Card Design Specifications. Version 2.0 (2005).⁴ You can obtain a copy of this standard from AAMVA on-line at <http://www.aamva.org> or by contact AAMVA at 4301 Wilson Boulevard, Suite 400, Arlington, VA 22203. You may inspect a copy of this standard at the Department of Homeland Security, 1621 Kent Street, 9th floor,

³ 73 FR 8279.

⁴ This document is currently being revised. The updated version will replace the current reference of Version 2.0 (2005) once finalized, and is expected to be labeled Version 1.0 (2009).

Rosslyn, VA (please call 703.235.0709 to make an appointment) or at the National Archives and Records Administration (NARA).

4. AAMVA DL/ID Security Framework; American Association of Motor Vehicle Administrators; February 2004. You can obtain a copy of this standard from AAMVA by contacting AAMVA at 4301 Wilson Boulevard, Suite 400, Arlington, VA 22203.
5. American National Standards Institute (ANSI)/North American Security Products Organization (NASPO) SA-v3.0P-2005; Security Assurance Standards for the Document and Product Security Industry. You can obtain a copy of this standard at <http://www.naspo.info>.
6. CFR Title 49 Transportation, Part 1520 Protection of Sensitive Security Information. You can obtain a copy of this standard at http://www.access.gpo.gov/nara/cfr/waisidx_06/49cfr1520_06.html.
7. Federal Specification FF-L-2740A; January 12; 1997. You can obtain a copy of this specification at https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/locks/dodlock_fedspecs.
8. Federal Information Processing Standard (FIPS) Publication (PUB) 199; Standards for Security Categorization of Federal Information and Information Systems; February 2004. You can obtain a copy of this standard at <http://csrc.nist.gov>.
9. FIPS PUB 200; Minimum Security Requirements for Federal Information and Information Systems; March 2006. You can obtain a copy of this standard at <http://csrc.nist.gov>.
10. NIST Special Publication 800-53; Revision 2; "Information Security"; December 2007.
11. Privacy Impact Assessment (PIA) for the REAL ID regulation; January 11, 2008. The PIA can be found at <http://www.dhs.gov/realid>.
12. International Civil Aviation Organization (ICAO) 9303, "Machine Readable Travel Documents," Volume 1, Part 1, Sixth Edition, 2006. You may obtain a copy of ICAO 9303 from the ICAO, Document Sales Unit, 999 University Street, Montreal, Quebec, Canada, H3C 5H7, or through email at sales@icao.int. You may inspect a copy of this standard at the Department of Homeland Security, 1621 Kent Street, 9th floor, Rosslyn, VA (please call 703.235.0709 to make an appointment) or at the National Archives and Records Administration (NARA).

The DHS REAL ID Office will make these documents and standards available upon request.

Please also refer to the definition section at the end of this document, Appendix B.

2 SECURITY MATRIX

<i>Threat</i>	<i>Vulnerability</i>	<i>Resolution</i>
2.1 <i>Theft of sensitive components</i>		
	Unauthorized persons may break in while facilities are closed and steal sensitive components.	• Provide physical security for the facility. See section 3.1. • Store sensitive components in secure containers or rooms. See section 3.1.2. • Provide Security Awareness Training. See section 3.5.2.3.
	Unauthorized persons may surreptitiously enter while facilities are open and steal sensitive components.	• Provide access control to secure areas. See section 3.2. • Store sensitive components in secure containers or rooms. See section 3.1.2. • Provide security awareness training. See section 3.5.2.3.
	Employees may pilfer sensitive components.	• Perform employee background checks. See section 3.5.1. • Provide access control to secure areas. See section 3.2. • Maintain good inventory control. See section 3.4.3.1.
	Visitors may pilfer sensitive components.	• Maintain visitor control. See section 3.2.5. • Provide access control to secure areas. See section 3.2. • Use employee badges. See section 3.2.1. • Provide security awareness training. See section 3.5.2.3. • Maintain good inventory control. See

		section 3.4.3.1.
	Sensitive components may be pilfered during manufacture and shipping.	• Maintain a secure supply chain. See section 3.4.3.2.
	Sensitive materials may be illegitimately recovered from production waste and spoilage.	• Destroy waste and spoilage. See section 3.4.3.3.
2.2 Theft of manufacturing or production equipment		
	Unauthorized persons may break in while facilities are closed and steal equipment.	• Provide physical security for the facility. See section 3.1. • Protect equipment. See section 3.1.3. • Provide security awareness training. See section 3.5.2.3.
	Unauthorized persons may surreptitiously enter while facilities are open and steal equipment.	• Provide access control to secure areas. See section 3.2. • Protect equipment. See section 3.1.3.
	Employees may steal equipment.	• Perform employee background checks. See section 3.5.1. • Protect equipment. See section 3.1.3.
	Visitors may steal equipment.	• Maintain visitor control. See section 3.2.5.6. • Use employee badges. See section 3.2.1. • Provide security awareness training. See section 3.5.2.3. • Protect equipment. See section 3.1.3.
	Equipment may be stolen during manufacture, shipping and storage.	• Maintain a secure supply chain. See section 3.4.3.2.

2.3 <i>Unauthorized access to Personally Identifiable Information</i>		
	Employees may access records containing PII for other than official business.	• Perform employee background checks. See section 3.5.1. • Provide security awareness training. See section 3.5.2.3. • Ensure IT Systems and Data Storage Security. See section 3.3.1. • Maintain internal audit controls. See section 3.7.
	Visitors may gain access to PII.	• Ensure IT Systems and Data Storage Security. See section 3.3.1. • Maintain visitor control. See section 3.26. • Provide security awareness training. See section 3.5.2.3.
	PII may be recovered from waste and spoilage.	• Destroy waste and spoilage. See section 3.4.3.3.
	PII may be recovered from media used in the issuance process but no longer needed.	• Destroy media when no longer needed. See section 3.3.3.

3 BEST PRACTICES

The section provides best practice recommendations for the security of REAL ID DL/IDs manufacturing, production, enrollment and issuance activities. Topics covered include the physical security of manufacturing, production and storage facilities; access control; security of PII; card design and security; personnel security; emergency/incident response planning; and audit controls. Before beginning security upgrades to its security, DHS strongly recommends that a State conduct a thorough gap analysis comparing its current security posture to these best practice recommendations prior to completing their REAL ID security plan.

These best practices are provided as guidance (or potential recommended solutions) to meet REAL ID security plan requirements. A State may choose a different method, practice, or approach. If a State chooses an alternative approach to meet the security requirements, the selected alternative should be as good as or better than the approach described in this document. DHS will examine the alternative procedure as part of the certification review.

States should conduct due diligence reviews for all service providers and contractors associated with these security services.

3.1 *Physical Security*

The best practices in this document will provide the States with suggestions for how to meet the needs of different types of facilities, due to the wide variety of environments in which card production facilities may be located. These best practices are a baseline suggestion, and will assist a State in determining how best to secure a particular facility. A State may use an alternative to the practices described in this handbook provided DHS deems that the alternative provides a level of security at least as good as or better than what is described in this document. A State wishing to use an alternative procedure to secure its facilities may wish to consult with DHS prior to the actual modification or construction of those facilities.

3.1.1 *Facility Access*

Unescorted access to facilities involved in the enrollment, issuance, manufacturing and production of REAL ID DL/IDs should be limited to covered employees.⁵ [The REAL ID regulation uses the term “covered employees” to describe all persons who are involved in the manufacture or production of REAL ID driver’s licenses and identification cards, or who have the ability to affect the identity information that appears on the driver’s license or identification card, or current employees who will be assigned to such positions.] Motor vehicle administration staff, that are not covered employees, should not have unescorted access to areas where REAL ID DL/IDs are manufactured, produced, or issued or to where customer PII is accessible.

⁵ The term “issuance” with respect to unescorted access refers throughout this document to areas where the ability to affect identity information on a DL/ID could be compromised. This does not refer to a sitting area, where individuals applying for a DL/ID might be waiting.

During operating hours, an access control system should be used, and the facility should be staffed by at least two covered employees at all times. During hours when the facility is not in operation, it should be secured using high security locks, intrusion detection alarms, surveillance cameras, and/or other barriers, as needed.

The actual physical security measures implemented at each facility may differ from location to location, as some facilities may be free-standing, and others may be located in the office buildings, shopping malls or industrial parks for example. Each facility should be surveyed and the physical security measures fitted to its specific operations and environment.

3.1.1.1 Perimeter walls

The survey of the facility should begin by determining the perimeter of the area. The perimeter walls could be walls that are either exterior or interior walls of the building in which the facility is located.

A perimeter wall of the facility should extend from the true floor to the true ceiling. If it does not, then security bars or another similar barrier should be installed to close any opening large enough for a person to pass through. As an alternative, the space below a raised floor or above a false ceiling may be secured using motion sensing, infrared intrusion detection sensors or other secure methods.

Perimeter walls should preferably be constructed of a material that is difficult to break through, such as concrete or masonry. If they are made of a less substantial material such as dry-wall, then they should be strengthened with steel mesh or other similar material. As an alternative, covering the interior of the facility with motion sensing or infrared intrusion detection sensors greatly reduces concerns about the type of material used to construct the walls.

3.1.1.2 Doors

Perimeter doors should be of heavy metal, solid wood or other reinforced secure materials. In many cases, fire safety regulations will require these doors to swing outward, meaning the hinge pins will be on the outside of the secure area. If this is the case, the door should have high security hinges so the hinge pins cannot be removed.

3.1.1.2.1 Entry/Exit Doors

These are the doors routinely used to enter and exit the facility. During the hours when the facility is closed, these doors should be locked. When the facility is in operation, these doors should be controlled using one of the access control methods described in Section 3.2. Each of these doors should include a mechanism to ensure the door automatically closes and maintains a tight, locked seal until accessed.

3.1.1.2.2 Loading Docks

Some larger facilities may have a loading dock or similar entrance used to bring supplies into the facility. These entrances should also be fitted with security doors. Except when actively engaged in the transfer of material into or out of the facility, these doors should be kept closed and locked. Whenever the door is open, a covered employee member or a guard should maintain constant surveillance of the doorway to assure access control is maintained.

3.1.1.2.3 Emergency Exits

Emergency exits should always go from inside the secure facility to outside. The inside (the side facing into the secure facility) of an emergency exit should have a “panic bar” or similar hardware. The outside of an emergency exit should have no door opening hardware. Emergency exit doors should be armed with an audible alarm that can be heard throughout the secure facility whenever the door is opened.

3.1.1.2.4 Locks

Locks are used to secure the facility when it is not in use. All entry/exit doors should have high security locks that are moderately resistant to skilled manipulation. One way to ensure the adequacy of locks used on entry/exit doors is to use locks that either meet the requirements of Federal Specification FF-L-2740A or are Underwriters Laboratories (UL) approved Group 2M locks. It is important not only to use secure locks but also to ensure they are properly installed. The standard locking mechanism used on many loading dock doors may need to be replaced with a more secure one. The loading dock door should only be capable of being unlocked from inside the secure area.

3.1.1.3 Windows

Any window that is large enough for a person to pass through should be secured. One option is to secure the opening using security bars. Another option is to alarm the windows using intrusion detection sensors. A third alternative is to use glass blocks or other specially designed high security glass. In some cases, the simplest solution may be to enclose the window opening with masonry material, i.e., concrete or security bars. As a final alternative, a well designed intrusion detection system using motion sensing, infrared intrusion detection sensors or other secure alternatives may provide adequate protection.

3.1.1.4 Air Ducts and Other Openings

The perimeter walls, floors, and ceilings of the secure facility should be checked for any air duct or other opening large enough for a person to pass through. Any such opening should be secured. One way to do this is to secure the opening using security bars. An alternative is to use intrusion detection sensors.

3.1.1.5 Intrusion Detection Systems

A good intrusion detection system depends as much on what happens when the alarm activates as it does on the quality of the components of which it is comprised. Careful selection and installation of the components should be matched with effective procedures for the monitoring of the system.

3.1.1.5.1 Sensors

A large variety of sensors are available for use in securing a facility. The actual choice of the best sensors for a given facility will depend on the use and construction of the facility. In general, sensors fall into one of two types. One type of sensor is to detect an attempt to enter an opening through the perimeter of the facility, such as a door or window. Examples of this type include magnetic door switches or glass break sensors. The other type of sensor is meant to detect the presence or movement of a person through space. An example of this type is the

infrared sensor. A combination of these two types of sensors usually provides the best protection.

Intrusion detection sensors should have battery back up to keep functioning for at least 24 hours during a power outage. The intrusion detection system should recognize if a sensor completely loses all power and should activate an alarm. Each sensor should also have anti-tampering capability such that any attempt to open or disable the sensor activates the alarm.

3.1.1.5.2 Control Panels and Keypads

An intrusion detection system typically operates from a control panel. Control panels should be installed within the secure facility. The control panel itself should be equipped with a sensor so that it activates whenever the panel is opened. The control panel should be provided with battery back up to allow it to remain in service for at least 24 hours during a power outage. The control panel should also have the capability to recognize if any sensor is no longer active and register an alarm.

Keypads for activating and deactivating the alarms should be located inside the protected area they control. These keypads should have anti-tampering sensors to detect any attempt to tamper with them and activate an alarm.

3.1.1.5.3 Monitoring

The intrusion detection system should have a monitoring service that provides constant monitoring twenty-four hours a day, seven days a week. This monitoring service may be performed either by a government entity or a commercial service. DHS recommends that, if a commercial service is used, the State should exercise due diligence to ensure that the selected service provider has a proven track record of dependability and reliability.

3.1.1.5.4 Response Force

What happens when an alarm is activated is one of the most important aspects of an effective intrusion detection system. Ideally, when the monitoring service recognizes the alarm has activated, it should immediately notify the response force. This response force may be either state or local law enforcement or a commercial service. Once the response force is notified, the monitoring service should then contact a covered employee using a contact list provided by the organization that manages the secure facility.

3.1.1.6 Cameras

The use of video cameras can be an effective security measure, and even more effective when used in combination with motion sensing capability. Cameras are effective for monitoring perimeter walls, secure storage and production areas on a daily basis. Video cameras should always be connected to a recording device for replay.

Note: The replay function should never displace the live picture on the screens routinely used for monitoring.

Video cameras can also be used in a “record-only” mode for areas that are not high-traffic areas or when the facility is closed. Cameras that are used in a record-only mode should have sufficient recording capacity to cover the longest period of time that the facility will be not be staffed. For example, if the facility is only open on Tuesdays and Thursday, the recording

capacity should be sufficient to cover the period from the close of the facility on Thursday until it is reopened on Tuesday. Ideally, recordings should be stored for a period of time and not immediately recorded over. This will allow for recordings to be reviewed when a possible incident is not discovered immediately. It is up to the State to determine how long such recordings should be kept.

3.1.1.7 Additional Information Regarding Over-the-Counter Facilities

The perimeter of an over-the-counter facility may be different during the time when it is open for business than it is when the facility is closed. During business hours, parts of the DL/ID office may be open to the public and just the area used for card production, issuance, and storage of PII may be a secure area. When the facility is closed, however, it may prove more economic to secure the entire office rather than just the area where card production occurs or PII is stored. This would allow the use of less substantial walls and doors to separate the general office area from the secure area.

If this approach is used, whenever the office is open the card production and PII storage areas should be under the constant observation and control of covered employees.⁶ There should never be a time when the office is occupied, without a covered employee present, even by other employees, to observe and control the secure area. This approach strongly relies on the covered employees to deter and detect any attempt at unauthorized entry into the secure area. In addition, it recommends that covered employees escort and observe any authorized visitors to areas where cards are produced or PII is stored.

3.1.1.8 Additional Information Regarding Continuous Production Operations

Some large production facilities may operate on a continuous basis, meaning covered employees are always present in the facility. In some cases, perimeter security and intrusion detection systems are less needed in a continuous operations facility. The most thorough approach would utilize a variety of the security monitoring techniques (cameras, people, sensors, etc.) in a compatible manner for the entire operation. The determining factor is the number of covered employees present in comparison to the size and layout of the facility.

If a sufficient number of covered employees are always present to maintain effective observation and control of the entire secure production facility, then the construction material used for the perimeter of the doors and walls need not be as substantial. A method of providing access control will still be needed. For facility areas under continuous effective observation and control, motion sensing or infrared intrusion detection sensors are not necessary at all times and may be limited. In a continuous operation facility, the covered employees should escort and observe any authorized visitors through the facility. This means that if visitors are present, enough covered employees should be available to handle card production activities and to provide escorts.

⁶ Effective observation and control means that it is highly unlikely that an unauthorized person could enter or remain in the secure area without being promptly detected.

In cases where covered employees are only able to effectively observe and control one part of a production facility at a time, it is best to utilize a variety of techniques (such as cameras and sensors) for the portions of the facility not under constant observation by the covered employees. For example a covered employee may have responsibility to monitor the production area during a period of time and therefore would not be able to observe the loading dock and storage room at the same time. In such a case, other security techniques should be employed to monitor the loading docks and storage room.

3.1.1.9 Fire Safety Considerations

The design of the facility should comply with all applicable fire and safety laws and regulations. However, fire and safety provisions should be complementary and not contradictory to the goal of providing security. For example, if the facility is located in a building that also has non-secure areas, the spaces should not be laid out so that people in the non-secure area need to pass through the secure area to exit the building during an emergency. If a State encounters a situation in which it appears that fire and safety requirements cannot be harmonized with physical security requirements, then it should contact the REAL ID Program Office at the Department of Homeland Security at (202) 447-3836 or email address, REALID@HQ.dhs.gov, for additional guidance and assistance.

3.1.2 Storage of Sensitive Components

The sensitive components used to manufacture or produce REAL ID DL/IDs should be protected at all times. These sensitive components should be stored in secure containers or in a specially constructed secure storage room. Only as much of the sensitive component as is needed for current production and issuance activities should be taken from the secure storage room at any given time. An accurate and up-to-date inventory of materials should be maintained. For example, facilities may choose to maintain a chain of custody log for sensitive components removed from secure storage areas for purposes of production or distribution. When the facility is closed, all sensitive materials should be removed from production equipment and stored in secure containers or rooms.

3.1.2.1 Secure Storage Containers

Security containers for the storage of sensitive components should provide at least ten minutes of protection against forced entry and have a lock that is moderately resistant to skilled manipulation. One way to ensure the adequacy of the security is to use security containers that either have an UL TL-15x6 rating and a UL class 2M lock or are U.S. General Services Administration (GSA) approved Class 5, or equivalent. These containers should be kept locked except while materials are being placed into them or removed from them. Recommend these containers be protected with intrusion detection sensors that are activated when the production facility is closed.

3.1.2.1 Construction of Secure Storage Rooms

Secure storage rooms should be constructed of solid concrete, steel plate, hardened steel mesh, or other material that would offer a similar level of protection. The walls should run from the floor to the ceiling of the secure room. This secure storage room should have a door at least as substantial as the walls and be fitted with a high security lock that is moderately

resistant to skilled manipulation, such as a lock that either meets the requirements of Federal Specification FF-L-2740A or is UL approved Group 2M. A better alternative is to use a GSA approved Class 5 vault door or equivalent. If this primary door is unlocked for any extended period of time, access to the area should be controlled with an entry/exit door as described in section 3.1.1.2.1, including the provision of access control. The primary door of the secure storage should have a door opening sensor connected to the intrusion detection system and the inside of the secure area should be covered with motion sensing or infrared intrusion detection sensors. Any opening through the perimeter, such as an air duct, should be secured using hardened steel bars, mesh or alternatives methods that provide at least the same or greater level of protections. Recommend large secure storage rooms not contain windows.

The design of the secure storage room should consider the safety of the people using it, such as fire safety codes. In addition, provision should be made for a person inadvertently locked inside to be able to open the door from the inside.

3.1.2.2 *Over-the-Counter Production Facilities*

Smaller amounts of sensitive components, such as might be found in “over-the-counter” facilities, can best be stored in a security container located within the secure areas of a facility.

3.1.2.3 *Central Issuance Production Facilities*

The larger amounts of sensitive components kept on hand at a central issuance production facility may best be stored in a secure storage room. However, if the amount of sensitive components stored at the central issuance production facility is relatively small, it may be more efficient to store them in a number of secure containers. If a State uses central issuance production, it should do an alternative of analyses to determine the most cost effective approach.

3.1.2.4 *Centralized Receiving and Shipping*

States with multiple production facilities (at different locations) may operate a central facility for receiving large shipments of sensitive components from vendors and breaking them down into smaller quantities for distribution to the production sites. One alternative is to align/construct a facility to the same standards as a production or issuance facility, including a provision for secure storage containers. With this alternative, all of the sensitive material should be secured when covered employees are not present. Another alternative is to conduct this activity entirely within a vault-like storage room as described in section 3.1.2.1.

3.1.3 *Security of Production Equipment*

Specialized equipment used in the manufacturing and production of REAL ID DL/IDs should be protected from theft. Several ways are available to provide effective theft protection for specialized equipment. One way is for the firmware in the equipment to have a connection to the State’s production system in order for the equipment to function. Another method is the

use of a hardware key that should be inserted for the equipment to work.⁷ When not in operation, these hardware keys should be stored separately in a secure place. Finally, the equipment can be securely fastened in place and covered by alarm systems. Whenever the facility housing the equipment is not occupied, the alarm system should be activated. Especially if this last approach is used, care is necessary to ensure that spare equipment (e.g., equipment that is intended to be used as a backup in case the primary equipment fails) is stored securely.

When equipment of this type is no longer needed, care should be exercised in arranging for its removal and or destruction. In situations where the State is moving to a new card design, cards of the old design may still be in circulation for some time. For this reason, equipment used to produce the old card design will still be of value to counterfeiters. Therefore this equipment should be destroyed or at least permanently disabled prior to disposal.

3.1.4 Contractor Facilities

The State may opt to have its REAL ID DL/IDs manufactured or produced in a facility operated by a contractor. If the State chooses to have its cards produced in a contractor operated and or owned facility, this facility should comply with the same REAL ID regulation minimum security requirements as does the State. A contractor may use the same facility to manufacture or produce REAL ID DL/IDs for more than one State. However, each State should maintain oversight of the contractor's manufacture or production of its own REAL ID DL/IDs.

If the contractor's facility is accredited at Level II of ANSI/NASPO-SA-v3.0P-2005, DHS will deem that it provides all necessary physical security as long as that accreditation remains current. However, DHS does not require an ANSI/NASPO accreditation. As an alternative, the State may establish its own procedures for insuring the contractor's facilities are secured. In this case, the State's comprehensive security plan should include the same information for the contractor facility as it would if the facility was operated by the State.

3.2 Access Control

3.2.1 Employee Badges and Credentials

Badges or similar credentials should be used to differentiate covered employees from other personnel who do not have authorized access into the facility. The use of badges can serve not only as an effective part of the access control system, but also as a way for covered employees to identify someone who should not be in the secure area.

If employee badges are used for covered employees, they should be distinctive from the badges of other personnel in the area – enough to allow discernment from several feet away. The badge for a covered employee could either be a variation of the regular employee badge or a completely separate badge. This allows for the immediate recognition that someone who is not authorized or has unescorted access is in the secure area. These badges should never be used

⁷ These hardware keys are sometimes called "dongles." These must be inserted in order for certain software or firmware to work. Since the associated equipment is rendered inoperable without the hardware key, equipment protected this way is of little value if stolen.

for making a decision to permit entry into the secure area without a close-up examination of the badge.

3.2.2 *Guards*

The use of guards to control access to the secure facility can be very effective. If guards are used, the guard should be positioned so that he or she can maintain visual control of the entry/exit door, or a video camera can be used to provide the guard the ability to maintain visual control of the entry/exit. There should be a door or turnstile controlled by the guard to allow entry into the facility.

If a badge system is used, the guard should be able to closely examine the badge and compare it to the badge holder before permitting access. If badges are not used, the guard should check another form of identification.

3.2.3 *Control by Staff*

In very small facilities, such as may be found in over-the-counter operations, entry into the secure facility can be controlled by the covered employees. In this case, a person wishing to enter the facility could, for example, use a buzzer or some other means to alert the covered employees within the secure facility to come to the door. In this arrangement, the entry/exit door should only be opened from the inside of the secure facility during the hours the facility is open for operation.

3.2.4 *Automated Systems*

A variety of automated devices are available for controlling access to the secure facility. These range from cipher locks to biometrics systems. The use of key card readers by themselves is not recommended since a lost or stolen card can be used by anyone to gain access to the secure facility. However, the use of a card reader in conjunction with a cipher or biometric can be very effective.

3.2.4.1 *Cipher Locks*

Cipher locks may be either mechanical or electric. The combination should be changed whenever a person who knows the cipher lock is removed from authorized access to the facility. Even when no one has been removed from access, the cipher lock combination should be changed periodically. The cipher lock's combination should never be given to a person who is not authorized access to the secure facility.

3.2.5 *Controlled Access to Terminals and Data Storage*

Physical access to the terminals used to enter data into the REAL ID customer enrollment and card issuance process and the electronic devices used for data storage of PII should be controlled. In many cases, the terminals and data storage will be located outside any secure production or storage facility and the access control need not be as rigorous. However, unescorted physical access to these areas should be limited to those whose duties necessitate them to have access. Please refer to section 3.3.1 for more guidance on Information Technology systems and data security.

3.2.6 *Visitor Control*

All visitors to the secure facility should be escorted by covered employees at all times while in the secure facility. A written log book should be kept of the visitors and the dates and times of their visits. Maintenance and janitorial personnel, including vendors, who have unescorted access to secure facilities where REAL ID DL/IDs are manufactured, produced, or issued, will require a similar check as covered employees, including the background check, in order to have such access. Without the background check, they should be considered as visitors.

3.3 *Security of Personally Identifiable Information*

The “Best Practices for the Protection of Personally Identifiable Information Associated with State Implementation of the REAL ID Act,” was originally included as an attachment to the Privacy Impact Assessment for the REAL ID regulation which DHS published on January 11, 2008. The State should refer to this document for guidance in developing a set of safeguards for the PII it collects, processes, and stores as part of its REAL ID compliance. The State should consider these best practices as minimum requirements to protect personally identifiable information.

3.3.1 *Information Technology Systems and Data Storage Security*

The information technology (IT) systems used to support the issuance of REAL ID DL/IDs includes all application processing, document verification, card production, and storage of PII and digital images of applicants and their documents. Based on the categorizations found in FIPS 199, the potential impact of these IT systems is considered to be “moderate.” Suitable controls as defined for the moderate-impact baseline of NIST Special Publication 800-53, Revision 1 should be used to secure these systems. Also note that persons who have access to these systems and its associated data storage are considered “covered persons” as defined by §37.45 of the REAL ID regulation, and will need a background check.

3.3.2 *Laptops and Portable Storage Media*

Preferably, laptop computers used to store or process PII and digital images of applicants and their documents should not be taken from State controlled workspaces. Data files containing PII and digital images that are stored on laptop computers should be encrypted.

If any PII or digital images of applicants or their documents are stored on any portable media, that media should be carefully controlled and detailed inventory records maintained. Additionally, the PII should be encrypted on the portable media device.

3.3.3 *Destruction of Media Containing Personally Identifiable Information*

When no longer needed, media containing PII should be destroyed.⁸ This includes not only waste paper but also electronic media such as disk drives and compact discs (CD). Paper products can be shredded or pulped. A number of different methods are available for cleansing magnetic media, including overwriting, degaussing, and mechanical destruction. The best

⁸ State laws, rules, regulations, and operations should be used to determine when media containing personally identifiable information are no longer needed.

method is often dependent on the type of media. The important thing is to ensure that the PII cannot be recovered.

3.3.4 Privacy Policy and the Fair Information Practice Principles

The State should develop and publicize a privacy policy that explains its commitment to meeting the following Fair Information Practice Principles:

3.3.4.1 Principle of Transparency

This principle requires that the State not be secretive about its use of PII and take the initiative to disclose its policies regarding its collection, use, dissemination, and maintenance.

3.3.4.2 Principle of Individual Participation

This principle requires the State, to the extent practical, allow the individual to determine what PII the State has concerning them, to access the data, and to seek correction of information the individual believes is erroneous.

3.3.4.3 Principle of Purpose Specification

This principle requires the State to specify the authority which permits it to collect PII and the purpose for which it will be used. It also requires a commitment not to use the information for reasons other than those stated at the time of collection.

3.3.4.4 Principle of Minimization

This principle requires the State only to collect the minimum PII necessary to accomplish the specified purpose.

3.3.4.5 Principle of Use Limitation

This principle requires the State only to use the PII collected for the specified purpose unless the individual agrees or the use is otherwise authorized by law.

3.3.4.6 Principle of Data Quality and Integrity

This principle calls on the State to ensure, to the extent practical, that PII is accurate, relevant, timely, and complete, within the context of each use.

3.3.4.7 Principle of Security

This principle requires the State to ensure that the PII it collects and uses is protected by reasonable security safeguards against loss or unauthorized access, destruction, misuse, modification, or disclosure.

3.3.4.8 Principle of Accountability and Auditing

This principle requires the State to make itself accountable for complying with all of the Fair Information Practice Principles, the privacy policies related to the implementation of the REAL ID Act of 2005 and its implementing regulation, and to provide training for its employees and contractors who use PII. It also requires the State to audit the actual use of PII.

3.3.5 Privacy Impact Assessment

The “Best Practices for the Protection of Personally Identifiable Information Associated with State Implementation of the REAL ID Act” recommends the State develop a Privacy Impact Assessment that addresses the following:

- What information is to be collected
- Why the information is being collected
- How the DMV intends to use the information it collects
- With whom the DMV will share the information it collects
- What notice or opportunities for consent will be provided to individuals regarding what information is collected and how that information is shared
- How the information will be secured

3.4 REAL ID DL/ID Design and Security

3.4.1 Choosing Security Features

In §37.15 the REAL ID regulation requires the use of an integrated set of security features to provide security for REAL ID DL/IDs. This means that the design should use a suite of Level 1, Level 2, and Level 3 security features that work together to protect against efforts to do the following:

- Counterfeit, alter, simulate, or reproduce a genuine document
- Alter, delete, modify, mask, or tamper with data concerning the original or lawful card holder
- Substitute or alter the original or lawful card holder's photograph and/or signature by any means
- Create a fraudulent document using components from legitimate driver's licenses or identification cards

Annex C of the AAMVA Card Design specifications provides an excellent list and description of card security features available for use. However, it is difficult to keep such a list current as new features enter the market. Although it is not definitive, it is a good starting point resource for States to use when investigating the subject.

It is strongly recommended that when procuring card security features, a State require the bidders to develop and present well integrated designs that protect against potential threats and have security features at all three levels.

(Note: Note that full descriptions of the card design and its security features are considered SSI and treatment of such information in accordance with section 5, Handling of Sensitive Security Information, should begin at the procurement phase. In addition, information about Level 3 features should always be handled on a strict "need to know" basis.)

Some card security features, if used together on the same card, have the effect of canceling out the intended security benefits. Therefore, bidders should be able to indicate that the integrated design avoids that pitfall.

3.4.1.1 Level 3 Physical Security Features

The following information should be considered at a minimum when choosing a Level 3 physical security feature.

- Tools to discern the feature are "expensive"/not widely available equipment. As examples: high resolution microscope/scanning electron microscope, high-powered

compound microscope, or chemical analysis equipment. Examples are not limited to those listed.

- Forensic Analysis by an expert is necessary. The feature requires someone trained in that feature to discern or identify it – this is to thwart people wanting to duplicate the document versus simulate it.
- The location of the feature is unknown to all but a few key officials, on a need-to-know basis. In order to locate the feature, someone would need to tell you where to look.
- The feature cannot be verified when someone presents a card for visual verification.

Please note that over time, some physical security features made be re-classified from a Level 3 to a Level 2 feature, as technologies become more widely available to the public. For example, the forensic ink taggant was previously considered by experts in the field of fraudulent document recognition to be a Level 3 feature. It is now is considered to be a Level 2, as handheld readers were developed to read the feature and are more easily available to the public.

3.4.2 *Serialized Card Bodies*

REAL ID DL/IDs should be produced from serialized card stock with preprinted inventory control numbers. The use of serialized card stock means that the card bodies will always be considered as sensitive components.

3.4.3 *Handling of Sensitive Components*

3.4.3.1 *Inventory Control*

For items with individual inventory control numbers, routine inventory records should indicate the numbers of each item received, on hand, used, wasted, and destroyed. If any items are found to be missing, the records should allow a determination of at least the range of numbers into which the missing items fall. Items such as ink should be controlled by the appropriate unit of measures (e.g., liters) used for shipment and storage. The inventory records should be sufficiently detailed to determine the amount of the material received, on hand, used, wasted, and destroyed. If sensitive components are unaccounted for then a report should be made to the appropriate law enforcement entity.

3.4.3.2 *Secure Supply Chain*

The State should ensure that sensitive components are provided via a secure supply chain. Sensitive components should only be obtained from reliable sources. The State should ensure that sensitive components are stored and handled by suppliers with the same care as exercised by the State itself. One recommended approach that States can use is to ensure its suppliers comply with the Level II requirements of the ANSI/NASPO-SA-v3.0P-2005 standard. However, DHS does not require that suppliers have an ANSI/NASPO accreditation. As an alternative, the State may establish its own procedures for ensuring the supplier provided adequate security.

3.4.3.3 *Destruction of Waste and Spoilage from the Production Process*

The waste and spoilage material, which card production inevitably generates, provides a double-barreled risk. First, it could be possible for someone to illegitimately recover sensitive components from the waste and spoilage. Second, it also could be possible for someone to

obtain unauthorized access to PII from the waste and spoilage. For this reason, the waste and spoilage material should be safeguarded.

Waste and spoilage material should always be stored in a secure area while it awaits destruction. Good inventory records should be kept to indicate how much waste and spoilage has been generated, how much is in storage, and when, how, and by whom it was destroyed.

Waste and spoilage material should be destroyed to a sufficient degree that sensitive components or PII cannot be recovered from the remnants. In many cases, a good quality cross-cut shredder will suffice. However, in some cases alternative methods may work better. States should consult with the vendor who designed the card about the best way to destroy the waste and spoilage resulting from the production process.

3.4.4 *Monitoring Document Security and Integrity*

3.4.4.1 *Initial Review and Reporting*

The State should conduct a review of its REAL ID DL/ID design and submit a report to DHS with its certification for Full Compliance.⁹ The review should evaluate the ability of the design to resist compromise and document fraud attempts. The report developed by this review should be handled as Sensitive Security Information.¹⁰

3.4.4.2 *Subsequent Review and Reporting*

The initial report of the design review should be updated and submitted to DHS whenever a security feature is modified, added, or deleted.¹¹ The State may want to conduct periodic reviews even if the design has not changed since counterfeiters may have devised new ways to defeat a security feature. Updated reports on the card design should be handled as Sensitive Security Information.¹²

3.4.4.3 *Laboratory Testing*

Based on the report of the card design review submitted, DHS may request a State to provide DHS with examination results from a recognized independent laboratory experienced with adversarial analysis of identification documents. The report of these results should be handled as Sensitive Security Information.¹³

3.4.5 *Markings for Compliant DL/IDs*

Pursuant to §37.17 (n) of the REAL ID regulation, States are required to mark REAL ID DL/IDs with a DHS approved marking to indicate its level of compliance with the REAL ID regulation. This means that there will be different markings for cards issued during material compliance and full compliance. In this document, these cards are referred to as “compliant” cards.

⁹ 6 CFR 37.15(d), pg. 5276

¹⁰ See section 5, “Handling of Sensitive Security Information” for additional information.

¹¹ 6 CFR 37.15(d), pg. 5276

¹² See section 5, “Handling of Sensitive Security Information” for additional information.

¹³ See section 5, “Handling of Sensitive Security Information” for additional information.

3.4.5.1 General Design

The symbol for a Materially Compliant card is a .25 inch square Pantone 117 (or CMYK equivalent) colored .25 inch by .25 inch star using regular ink (approximately 6.35 mm by 6.35 mm). [CMYK = cyan, magenta, yellow, and key (or black).]

The same ink and size of the indicator will be used for both the “Materially Compliant” and the “Fully Compliant” cards, but the art work will be different. The size of the indicator will be .25 inch by .25 inch (approximately 6.35 mm by 6.35 mm).

The symbol for a Fully Compliant card is a .25 inch square Pantone 117 (or CMYK equivalent) colored .25 inch by .25 inch (approximately 6.35mm by 6.35mm) circle with a star cut out to reveal the background using regular ink.

3.4.5.2 Location

The compliant markings of the “star” or “star cut out” should appear on the face and the top third of a landscape or portrait card.

3.4.5.3 Security

The markings on both compliant and non-compliant cards should be secured in the same way that other personalization data on the card should be secured. For example, if the name, photo, etc. are secured using a high security overlay, then the marking should also be secured by the security overlay. Similarly, if the personalization data is printed using laser printing, then the marking should be laser printed on the card.

3.4.6 Marking Temporary or Limited-Term REAL ID DL/IDs

Pursuant to §37.21 of the REAL ID regulation, States may only issue a temporary or limited-term REAL ID DL/ID to an individual who has temporary lawful status in the United States and the State has verified that status with DHS. These cards should clearly indicate on their face and in the machine readable zone that they are temporary or limited-term REAL ID DL/IDs.

The temporary or limited-term REAL ID DL/ID should be marked on the front with the phrase “Temporary” or “Limited-Term” within the top third of the card. The specified font is Helvetica Bold with a recommended font size of 9 points, however not less than a 7 points font in regular black ink. This phrase should be secured in the same way that other personalization data on the card is secured.

3.4.7 Marking of Non-Compliant DL/IDs

Pursuant to §37.17 States wishing to comply with REAL ID may also choose to issue driver’s licenses and identification cards that are not acceptable by Federal agencies for official purposes. These cards should be marked on their face and in the machine readable zone (MRZ) to indicate they are not acceptable for any official purpose as defined in §37.3 of the REAL ID

regulation.¹⁴ For simplicity's sake, this document refers to such cards as "non-compliant" cards.

Non-compliant cards should state in the top third of the face of the card, being the same side with photo and printed data elements, "NOT FOR REAL ID PURPOSES." The specified font is Helvetica Bold with a recommended font size of 9 points, however not less than a 7 points font in regular black ink. This phrase should be secured in the same way that other personalization data on the card is secured.

3.4.8 *Encryption of the 2D Barcode*

The minimum information required in the 2D barcode is discussed in §37.19 of the REAL ID regulation, and there is no requirement in the regulation to encrypt this information. However, a state may choose to encrypt any additional data (e.g. biometrics) it adds to the 2D barcode beyond the minimum information required by REAL ID, provided the State ensures all law enforcement personnel have the ability to easily access the data included in the MRZ.¹⁵

3.5 *Personnel Security*

3.5.1 *Background Checks*

3.5.1.1 *Who Needs a Background Check?*

Pursuant to §37.45, States must conduct a background check for all covered employees. As stated earlier in the document, the term "covered employees" are all persons who are involved in the manufacture or production of REAL ID driver's licenses and identification cards, or who have the ability to affect the identity information that appears on the driver's license or identification card, or current employees who will be assigned to such positions. A "covered position" is a staff position that has duties assigned that are conducted by a covered employee. Any person (including a contractor or an employee assigned to another department within the State) who does any of the following activities would be considered a covered employee:

- Involved in the manufacturing or production of REAL ID DL/IDs
- Has unescorted access to secure facilities where REAL ID DL/IDs are manufactured, produced, or issued
- Handles sensitive components or has access to secure storage for sensitive components used in REAL ID DL/IDs
- Accepts or reviews REAL ID DL/ID applications or source documents
- Takes photos for REAL ID DL/IDs
- Inputs data from REAL ID DL/ID applications or source documents into the IT systems
- Is involved in the decision making process to determine if a REAL ID DL/ID is issued or the information that will appear on the card

¹⁴ MRZ in this document refers to the 2D PDF 417 barcode. States should consult the AMVA DL/ID Card Design Specifications Version 4.0 for the formatting of data in the MRZ.

¹⁵ The information stored on the barcode enables law enforcement officers to compare the information on the barcode with the information on the front of the card to determine whether any information on the front of the card has been altered and to automatically populate law enforcement reports.

- Has the ability to review, alter, or add any of the data items listed in §37.33 of the REAL ID regulation in the IT systems used to process and store data related to REAL ID DL/IDs
- Supervises or manages a “covered person” who performs any of these tasks

This list should not be considered exhaustive; States may determine additional staff positions as “covered positions.”

3.5.1.2 When Should the Background Checks Be Completed?

The program and procedures for conducting background checks should be developed and background checks underway by the time a State begins issuing REAL ID DL/IDs under Material Compliance. The background checks for all employees and contractors working in “covered positions” must be completed by the time a State enters Full Compliance. Before issuing REAL ID DL/IDs under Material Compliance, a State should reassign, temporarily, any person in a covered position whose background check has not been successfully completed.

3.5.1.3 What is Included in a Background Check?

A background check, at a minimum, includes the following:

- Employment references for any employee who has not been employed by the DMV for at least two consecutive years since May 11, 2006.¹⁶
- Name-based and fingerprint-based criminal history records check using the Federal Bureau of Investigation’s (FBI) National Crime Information Center (NCIC), and the Integrated Automated Fingerprint Identification System (IAFIS) and State repository records.
- Employment eligibility verification to ensure compliance with the requirements of section 274A of the Immigration and Nationality Act (8 U.S.C. 1324a) and its implementing regulations (8 CFR part 274A).

3.5.1.4 Disqualification

The REAL ID regulation, §37.45 (b) (1) (i), explains the situations under which a person may be permanently disqualified from serving in a “covered position.” Anyone who is permanently disqualified may never serve in a “covered position” and should not be involved in the manufacture or production of REAL ID DL/IDs or be able to affect the information that appears on a REAL ID DL/ID.

The REAL ID regulation, §37.45 (b) (1) (ii), explains the situations under which a person may be disqualified from serving in a “covered position” on an interim basis. A person who is disqualified on an interim basis should not be involved in the manufacture or production of REAL ID DL/IDs or be able to affect the information that appears on a REAL ID DL/ID until the period of interim disqualification has been completed.

¹⁶ While it is desirable to determine other information, such as why the employee left the previous position, many employers will provide only verification of the dates of employment.

Also pursuant to §37.45 of the regulation, the State may establish procedures to allow for a waiver of the regulatory requirements prohibiting placement of an employee in a covered position for an interim disqualifying offense. This procedure should be documented as part of the State's security plan.

The REAL ID regulation §37.45 (b) (1) (iii) explains that a person who is wanted or under indictment for a felony is disqualified until the want or warrant is released. This person may not be involved in the manufacture or production of REAL ID DL/IDs or be able to affect the information that appears on a REAL ID DL/ID as long as the want or warrant is in effect.

If the criminal background check reveals an arrest without disposition, the State should make a diligent effort to determine the disposition. The State may establish a procedure to waive the requirement for disqualification if it cannot determine the disposition of the arrest after having made a diligent effort. This procedure should be documented as part of the State's security plan.

3.5.1.5 Employee Rights

States should inform current and prospective employees who will serve in "covered positions" that they will undergo a background check and provide a description of what the background check will cover. If as a result of the background check an employee is disqualified, he or she should be informed and given a chance to appeal to the appropriate State or Federal government or otherwise challenge the findings of the background check.

3.5.2 Training

3.5.2.1 When Should Training Occur?

The Fraudulent Document Recognition (FDR) and security awareness training programs should be operational before the State begins issuing REAL ID DL/IDs under Material Compliance. All covered employees should complete training before the State begins issuing REAL ID DL/IDs under Full Compliance. Thereafter, all covered employees should receive refresher training on a recurring basis, at least once every three years. After full compliance is reached, new covered employees should receive all security training before or shortly after assuming their new duties.

3.5.2.2 Fraudulent Document Recognition Training

Pursuant to §37.41, all covered employees engaged in the handling of source documents or engaged in the issuance of REAL ID DL/IDs should receive FDR training. The REAL ID regulation states that the AAMVA FDR Training program is approved for this requirement. If the State wishes to use an alternative FDR training program it should contact the REAL ID Office at the Department of Homeland Security to obtain approval of that program. Employees who are not involved in the issuance decision making process, such as those who work in a central card production facility or in a data processing center, are not required to have FDR training.

3.5.2.3 Security Awareness

All covered employees should receive security awareness training. All covered employees should receive training that covers the threats to the security of the REAL ID DL/ID. This should include recognition of the threat, what actions they should take if they discover a security threat, and how to report it. Portions of this training may vary depending on the duties of the

employee. Covered employees should also be trained in the security measures, such as access control procedures, locks, intrusion detection alarms and emergency/incident plans, for the secure facility where they work. Employees who handle Sensitive Security Information should receive training in the handling of Sensitive Security Information.¹⁷

3.6 Emergency/Incident Response

Each secure facility should develop a response plan for emergencies or incidents that may occur at its location. At a minimum, these plans should cover fire, medical emergencies, bomb/bomb threat, and severe weather. Other incidents that the State may want to cover include earthquakes, terrorist incidents, and disgruntled employees. In the development of these plans, the safety of personnel is paramount.

The security interest in these plans is, to the extent possible, preventing loss of control of sensitive materials and equipment, or, in the aftermath, recovering control at the earliest practical time. For example, a good plan for a medical emergency would call for a covered employee to meet the emergency medics at the entry/exit door, escort them to the patient, observe without interfering, and then escort them back out of the facility. If sensitive components or specialized production equipment is found to be unaccounted for after an emergency or incident is complete, the senior person in charge of the facility should make a report to the appropriate state level police agency, the AAMVA Fraud Early Warning System and the DHS REAL ID Program Office.

3.7 Audit Controls

The State should maintain adequate audit trails. The ability to determine who performed a given action may be determined through the use of user accounts within the systems. An employee should only work on a workstation that he or she logged onto with his or her own user account. At a minimum, audit controls should do the following:

- Keep a record of when, where, and by whom the determination was made to issue the REAL ID DL/ID
- Each time personally identifiable data is accessed, keep a record of who made the access, when it was made, and from where it was made
- Each time personally identifiable data is changed, keep a record of who made the change, when it was made, and from where it was made, and what was changed
- For each REAL ID DL/ID produced, keep a record of where and when it was made and who was in charge of the process at that time

¹⁷ See section 5, “Handling of Sensitive Security Information” for additional information.

4 SECURITY PLAN

This section delineates the information that the State should include in the security plan pursuant to §37.41 of the REAL ID regulation. The security plan does not need to be a single, unified document. Instead, it can be made up of several plans, policies, and procedures that, taken as a whole, address all of the issues identified in this handbook. The parts of the plan that should be handled as Sensitive Security Information are indicated.¹⁸ For additional reference, the REAL ID Privacy Impact Assessment can be found at <http://www.dhs.gov/realid>.

4.1 Plan Contents

4.1.1 Physical Security and Access Control Methods (Handle as Sensitive Security Information)¹⁹

4.1.1.1 Information about Card Production Facility

For each secure facility used for the production of REAL ID DL/IDs or as a centralized shipping and receiving facility, provide the following information:

- Location of the facility
- Type of operation: central production or over-the-counter operation
- Frequency of card production
- Facility operating hours²⁰
- Authority that owns and operates the facility: State, local government entity, contractor, etc.
- If the facility is accredited under ANSI/NASPO-SA-v3.0P-2005 standard Level II, provide documentation showing proof of the accreditation and skip the remaining items²¹
- A statement that the facility follows the guidelines in this handbook for providing adequate physical security and that for each secure production facility the following documentation is maintained on file for review:
 - o Description of the construction of perimeter walls, true ceiling, and true floor, including whether the perimeter walls connect to the true floor and true ceiling. If they do not, explain how the gap is secured
 - o Description of the construction of the entry/exit doors, including the type of lock and the method of securing hinge pins
 - o Description of all loading dock doors, including the type of construction and the locking mechanism used
 - o Description of all emergency exits, including the type of material from which they are constructed, how the hinges are secured, and the type of locking mechanism used, and if an alarm activates when they are opened

¹⁸ See section 5, “Handling of Sensitive Security Information” for additional information.

¹⁹ See section 5, “Handling of Sensitive Security Information” for additional information.

²⁰ The Facility Operating Hours does not need to be handled as Sensitive Security Information.

²¹ DHS does not require ANSI/NASPO certification. However, if the facility has been certified, DHS deems the facility is secure and the State need not provide any information listed in paragraph 4.1.1.1 beyond proof of the certification.

- o Description of how any windows, air ducts, or other opening in perimeter walls are secured
- o Description of all access control methods and procedures
- o Description of all the intrusion detection systems, including the location of the control panel, location of keypads, and the type and location of each type of sensor
- o A drawing (need not be to scale) showing the location of the following:
 - All doors, windows and other openings through the perimeter walls
 - Location of intrusion detection system components
 - Location of sensitive component storage
- If the secure facility has storage containers for the storage of sensitive components, give the number of containers and the GSA rating of the containers.
- Explanation of how any sensitive equipment is secured

4.1.1.2 Information about Handling and Storage of Sensitive Components

The following information about the handling and storage of sensitive components should be included:

- Provide a list of the sensitive components used in the production of REAL ID DL/IDs.
- Provide a list of sensitive equipment used in the production of REAL ID DL/IDs.
- Document whether the sensitive components are stored in secure containers or in a secure storage room. If a secure storage room is used, provide the information from Section 4.1.1.3.

4.1.1.3 Information about Secure Storage Rooms

The following information about secure storage rooms should be included:

- Location of the facility
- Frequency of card production
- Facility operating hours
- Authority that owns and operates the facility: State, local government entity, contractor, etc.
- If the facility is accredited under ANSI/NASPO-SA-v3.0P-2005 standard Level II, provide documentation showing proof of the accreditation and skip the remaining items.²²
- A statement that the facility follows the guidelines in this handbook for providing adequate physical security and that for each secure production facility the following documentation is maintained on file for review:
 - o Description of the construction of perimeter walls, true ceiling, and true floor, including whether the perimeter walls connect to floor and ceiling of the secure room

²² DHS does not require ANSI/NASPO certification. However, if the facility has been certified, DHS deems the facility is secure and the State need not provide any information listed in Section 4.1.1.1 beyond proof of the certification.

- o Description of the construction of the door, including how the hinges are protected and the type of lock
- o Description of access control methods and procedures
- o Description of the intrusion detection system, including the location of the control panel, location of keypads, and the type and location of each type of sensor
- o A drawing (need not be to scale) showing the location of the following:
 - All doors, windows and other openings through the perimeter walls
 - Location of intrusion detection system components
 - Location of sensitive component storage

4.1.2 *Security of Personally Identifiable Information*

The following information on the security of PII should be included:

- A description of the administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the PII collected, stored, and maintained in DMV records and information systems for purposes of complying with the REAL ID Act, including the following information: (Handle as Sensitive Security Information) ²³
 - o Explanation of how the State prevents the unauthorized access, use, or dissemination of applicant information and images of source documents
 - o Description of the standards and procedures for document retention and destruction.
- Pursuant to §37.41 of the REAL ID Final, provide a copy of the State's Privacy Policy that covers the PII used in complying with the REAL ID Act. As recommended in the Best Practices, the Privacy Policy may address each of the following Fair Information Practice Principles:
 - o Principle of Transparency
 - o Principle of Individual Participation
 - o Principle of Purpose Specification
 - o Principle of Minimization
 - o Principle of Use Limitation
 - o Principle of Data Quality and Integrity
 - o Principle of Security
 - o Principle of Accountability and Auditing
- Provide a copy of the State's Privacy Impact Assessment for its DMV records and information systems, if the State chooses to conduct one.
- [After confirmation, the State must provide a statement indicating that the DMV has complied with the requirements of the Driver's Privacy Protection Act, 18 U.S.C. 2721 et seq regarding the release and use of PII collected and maintained by the DMV pursuant to the REAL ID Act.](#)

²³ See section 5, "Handling of Sensitive Security Information" for additional information.

4.1.3 Card Security Features (Handle as Sensitive Security Information) ²⁴

4.1.3.1 Description of Card

Provide a complete description of the design of the REAL ID DL/ID, including the security features.

4.1.3.2 Monitoring Document Security and Integrity

Provide a copy of the report that determined the REAL ID DL/ID design is resistant to compromise and document fraud attempts.

4.1.4 Biometrics Usage

If biometrics are used in conjunction with the issuance of REAL ID DL/IDs, then the following information should be provided:

- o State the type of biometric used (e.g., 2-d face, 3-d face, fingerprint, iris scan)
- o If a biometric is stored on the card, provide information about the technology used for storage and the format of the biometric
- o If a biometric is stored in a database, provide information about the format in which it is stored and how the biometric is linked to the rest of the data related to the individual
- o Describe how the biometric is used (e.g., identity verification, search for duplicates)
- o List any technical standards used in development or operation of the system

4.1.5 Personnel Security

4.1.5.1 Employee Credentials or Identification Badges

Describe what kind of credentials or identification badges are issued to:

- Covered employees, including how these badges differ from employees that are not “covered,” and
- Other staff.

4.1.5.2 Employee Background Checks

Provide a copy of policy, procedure, rule, or regulation documents that establishes a program of employees background checks pursuant to §37.45 of the REAL ID regulation.

4.1.6 Training

4.1.6.1 Fraudulent Document Recognition Training

Provide a copy of the policy, procedure, rule, or regulation that establishes the following:

- o Requirement for the training
- o Amount of time between refresher training sessions
- o The training program used (either the AAMVA program or a DHS approved alternative)
- o The percentage of covered employees who have received training in the last three years

²⁴ See section 5, “Handling of Sensitive Security Information” for additional information.

4.1.6.2 *Security Awareness*

Provide a copy of the policy, procedure, rule, or regulation that establishes the following:

- o Requirement for the training
- o Amount of time between refresher training sessions
- o An outline of the topics covered by the training
- o The percentage of covered employees who have received training in the last three years

4.1.7 *Emergency/Incident Response Plans*

Provide confirmation that for each secure facility there are emergency/incident response plans that cover, at a minimum, fire, medical emergency, bomb/bomb threat, and severe weather at the State's secure facilities. Additionally, provide confirmation that copies of these plans are available for inspection upon request.

4.1.8 *Internal Audit Controls (Handle as Sensitive Security Information²⁵)*

Describe how an audit trail is maintained and what data items are recorded for each of the following :

- o The determination to issue the REAL ID DL/ID
- o Each time PII is accessed
- o Each time PII is changed
- o Each REAL ID DL/ID produced

²⁵ See section 5, "Handling of Sensitive Security Information" for additional information.

5 HANDLING OF SENSITIVE SECURITY INFORMATION

The REAL ID regulation calls for States to handle certain information in accordance with the Code of Federal Regulations, Title 49 Transportation, Part 1520 Protection of Sensitive Security Information.²⁶ Please refer to the appendices for guidance on training and additional information related to the handling of SSI, in addition to the information included in this section. The REAL ID Program office encourages you to follow the best practices for successfully handling Sensitive Security Information and maintain an appropriate level of security for the Security Plans that will be generated as a result of this document.

5.1 *Information Designated as Sensitive Security Information*

Per Section 37.41 (C), the security plan required as a result of the regulation contains Sensitive Security Information and must be handled and protected in accordance with 49 CFR Part 1520. Sensitive Security Information is an information protection program providing storage and dissemination controls intended to prevent malefactors from obtaining information that would allow them to defeat or avoid security measures and equipment. In the context of REAL ID, Sensitive Security Information is information that deals with the physical security of the card production facilities and the security of the IT systems used to issue REAL ID DL/IDs, and the description and analysis of card security features, as determined by the State. The sections of the security plan that deal with the physical security of the card production facilities and the security of the IT systems used to issue REAL ID DL/IDs, and the description and analysis of card security features should be designated as Sensitive Security Information.

5.2 *Access to Sensitive Security Information*

Access to this information should be limited to covered employees whose duties result in a “need to know” and to their supervisors or managers.²⁷ An employee’s need to know or be able to access Sensitive Security Information is a clear indication that the employee is filling a covered position.

5.3 *Protection of Sensitive Security Information*

When handling or discussing Sensitive Security Information, employees should be conscious of their surroundings. Sensitive Security Information should only be discussed or shared with covered employees who have a need to know. Documents containing Sensitive Security Information should never be left unattended and should always be protected from unauthorized viewing. Appropriate security measures should be employed to ensure Sensitive Security Information sent via email, or other means, is only shared with authorized covered personnel who have a need to know. Such measures may include password protection of electronic files, limited network access, or encryption.

²⁶ This document is often referred to as 49 CFR Part 1520.

²⁷ The need to know has a broad application and personnel with a need to know may include a supervisor, manager, legal counsel, contractor and/or network administrator.

5.4 *Storage*

When not in use, Sensitive Security Information should be stored in a secure container, such as a locked desk or file cabinet or in a locked room. To prevent unauthorized access, users of computers which contain Sensitive Security Information should log out or turn off the computer when they are not in the immediate vicinity.

5.5 *Marking Documents SSI*

Documents that contain Sensitive Security Information, such as the REAL ID Security Plan, should possess a header on every page, including cover pages, reading "SENSITIVE SECURITY INFORMATION." Each document should also possess a footer on every page reading "WARNING: This record is controlled under 49 CFR 1520. Unauthorized release may result in a civil penalty.

5.6 *Destruction*

When papers or media containing Sensitive Security Information are no longer needed, a Covered Employee should destroy them to the extent that the information cannot be reconstituted or recovered.

6 APPENDIX A: ACRONYMS

Acronym	Definition
AAMVA	American Association of Motor Vehicle Administrators
ANSI	American National Standards Institute
CFR	Code of Federal Regulations
CMYK	Cyan, Magenta, Yellow or Key (black)
DHS	Department of Homeland Security
DMV	Department of Motor Vehicle
DL/ID	Driver's licenses and identification cards
FBI	Federal Bureau of Investigation
FDR	Fraudulent Document Recognition
FIPS	Federal Information Processing Standard
GSA	General Services Administration
IAFIS	Integrated Automated Fingerprint Information System
ICAO	International Civil Aviation Organization
IT	Information Technology
MRZ	Machine Readable Zone
NASPO	North American Security Products Organization
NCIC	National Crime Information Center
NIST	National Institute of Standards and Technology
OTC	Over-the-counter
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SSI	Sensitive Security Information

7 APPENDIX B: TERMS AND DEFINITIONS

Term	Definition
Compliant Card	A card issued in compliance with the requirements of the REAL ID Act and the final REAL ID regulations issued by DHS.
Continuous Operations	A facility is in continuous operations if it is <u>always</u> occupied by covered employees, including evenings, weekends, and holidays.
Covered Employee	An employee or contractor whose duties involve the manufacture or production of REAL ID DL/IDs, or who has the ability to affect the identity information that appears on a REAL ID DL/ID.
Covered Position	A staff position which requires a Covered Employee.
DL/ID	Driver's license and/or identification card.
DMV	The Department of Motor Vehicles (DMV) is an agency responsible for the issuance of driver's licenses and identification cards within a given jurisdiction.
Enrollment	Enrollment is the process of accepting, recording, and storing customer PII in a DMV facility.
Facilities	The locations where REAL ID DL/IDs are manufactured, produced, or issued; where applicants are enrolled and staff have access to customer PII.
Issuance	The delivery of personalized cards or credentials to individual customers via mail, over-the-counter, or by other means.
Level 1 physical security feature	Cursory examination, without tools or aids involving easily identifiable visual or tactile features, for rapid inspection at point of usage.
Level 2 physical security feature	Examination by trained inspectors with simple equipment.
Level 3 physical security feature	Inspection by forensic specialists.
Manufacturing	Production of the materials used to produce or personalize cards. This includes substrates, card blanks, laminates, security devices, and other physical components of the cards.
Non-compliant Card	A DL/ID issued by a REAL ID compliant State to a person that has not met the requirements for issuance of a REAL ID DL/ID. Such a card is not acceptable by Federal agencies for official purposes as defined in §37.3 of the REAL ID regulation.

Personally Identifiable Information	Any information which can be used to distinguish or trace an individual's identity, such as their name; driver's license or identification card number; social security number; biometric record, including a digital photograph or signature; alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as a date and place of birth or address, whether it is stored in a database, on a driver's license or identification card, or in the machine readable technology on a license or identification card.
Production	The physical production or personalization of individual cards in central issuance, over-the-counter (OTC) or hybrid facilities. Production takes the manufactured components of a card and produces an individualized credential.
REAL ID DL/ID	A driver's license or identification card produced in compliance with the REAL ID Act and the final REAL ID regulations issued by DHS.
REAL ID Regulations	Federal Register, Part II; Department of Homeland Security; 6 CFR Part 37; Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Final Rule; Federal Register / Vol. 73, No. 19 / Tuesday, January 29, 2008 / Rules and Regulations; pp. 5272-5340.
Sensitive Component	A component used in the production of a REAL ID DL/ID that contains special features that differentiate from similar components commonly available on the open market. The test for deciding if a component is sensitive is the determination that a person could make a "better" fraudulent document if he or she had the component. Since blank REAL ID DL/ID bodies must contain inventory control numbers, these blank card bodies are sensitive components.
Sensitive Security Information	Sensitive Security Information is an information protection program providing storage and dissemination controls intended to prevent malefactors from obtaining information that would allow them to defeat or avoid security measures and equipment. In the context of REAL ID, Sensitive Security Information is information that deals with the physical security of the card production facilities and the security of the IT systems used to issue REAL ID DL/IDs, and the description and analysis of card security features, as determined by the State.

8 APPENDIX C: SSI TRAINING GUIDANCE

Refer to the DHS “SSI Basic Training for U.S. Department of Homeland Security Stakeholders” for guidance on how to handle Sensitive Security Information.

U.S. Department of Homeland Security
Transportation Security Administration
Office of the Special Counselor
Sensitive Security Information Office
Presents:

**SSI Basic Training for U.S. Department
of Homeland Security Stakeholders**



Transportation Security Administration

Sensitive Security Information Office
Safely Sharing Information

1

SSI Basic Training

Objectives

This training will focus on:

- Differences between Sensitive Security Information (SSI) and the following three types of information:
 1. Classified National Security
 2. For Official Use Only (FOUO)
 3. Law Enforcement Sensitive (LES)
- Requirements and “Best Practices” for safely sharing and protecting SSI



Transportation Security Administration

Sensitive Security Information Office
Safely Sharing Information

2

SSI Basic Training

Brief History of SSI

Contrary to popular belief, SSI was not developed after September 11, 2001. Rather, it was in response to hijackings that occurred in the early 1970s.

The *Air Transportation Security Act of 1974*, required the FAA to establish a regulation for sharing sensitive information with airlines and airports. The FAA published the first regulation regarding SSI in the Federal Register in 1976.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

3

Sensitive Security Information (SSI) VS. Classified, FOUO, and LES Information



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

4

SSI Basic Training

All information held by the government falls into two categories:

- **Classified National Security Information**
(Confidential, Secret, Top Secret)
- **Unclassified**
(SSI, FOUO, LES, Public Information, etc.)



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

5

SSI Basic Training

Classified Information

"Official information which relates to national defense or foreign relations of the United States which has been deemed to require protection from unauthorized disclosure."*



Example:

A special ops mission gathers intelligence on terrorist operations. The intelligence information is classified.

* Source: TSA Office of Security



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

6

SSI Basic Training

Unclassified Information Falls into Two Categories

- Sensitive But Unclassified (SBU)

A broad category that includes both regulated and unregulated means of protecting information including information marked as SSI, FOUO, and LES

- Public Information

All other information



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

7

SSI Basic Training

Sensitive Security Information (SSI)

Information obtained or developed which, if released publicly, would be detrimental to transportation security.

Examples:

- TSA No Fly List and Selectee List
- Screening Standard Operating Procedures (SOPs) used by Transportation Security Officers (TSOs)
- Aircraft Operator Standard Security Program (AOSSP)



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

8

SSI Basic Training

For Official Use Only (FOUO)

Information not protected by regulation that could adversely affect a Federal program if publicly released without authorization.*

*Source: DHS Management Directive 11042.1

Example:

Security guard staffing schedules for production facilities.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

9

SSI Basic Training

Law Enforcement Sensitive (LES)

Documents marked as LES are intended for official use only. No portion of the document should be:

- Released to the media or the general public
- Posted to or sent via non-secure Internet servers

Release of LES material could adversely affect or jeopardize investigative activities.*

* Source: FBI's Web site

Example:

FBI Intelligence Bulletins



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

10

SSI Basic Training

What are the differences?

FOUO, LES, and SSI are all categories of Sensitive But Unclassified information, but:

- SSI is based on U.S. law and protected by a Federal regulation; FOUO and LES are not
- SSI protects information related to transportation security; FOUO and LES have no limitations on subject matter



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

11

SSI Basic Training

What Are the Differences? (continued)

- In litigation, SSI has stronger protections from court-ordered production requests than LES while documents marked only as FOUO have no protection at all
- SSI protections have been challenged numerous times in Federal court proceedings and SSI protections have always been upheld
- SSI is protected from public release under a Freedom of Information Act (FOIA) request; FOUO or LES may be either be protected or publicly released under FOIA



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

12

SSI Basic Training

What Are the Differences? (continued)

- Unauthorized SSI disclosure may result in a civil penalty; FOUO and LES breaches cannot
- Documents that contain SSI must be marked as SSI – not FOUO or LES: when information is pulled from reports marked LES, FOUO, and SSI, the new report must be marked as SSI
- If stakeholders have questions on marking or re-marking reports that contain SSI, they should contact the entity that created the SSI document



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

13

Focus on SSI Regulation



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

14

SSI Basic Training

16 SSI Categories

The Federal regulation (49 CFR Part 1520.5(b)) defines 16 categories that information must fall under to be protected as SSI. After each category is an example of information that would be protected under that category:

- (1) **Security Programs and Contingency Plans** – Security Plans (each airport and airline must have one and all are protected as SSI)
- (2) **Security Directives** – SDs are issued to airlines and airports pertaining to a wide range of security issues from access control to how to handle a positive match on the No Fly List



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

15

SSI Basic Training

16 SSI Categories (cont.)

- (3) **Information Circulars** – Notices issued by DHS or DOT regarding a threat to transportation security
- (4) **Performance Specifications** – Specifications for any checkpoint, checked baggage, and cargo screening equipment deployed at airports
- (5) **Vulnerability Assessments** – Assessments by DHS of any transportation asset (e.g., the nation's largest airports and maritime ports)



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

16

SSI Basic Training

16 SSI Categories (cont.)

- (6) **Security Inspection or Investigative Information** – Unplanned (incident or violation) inspection or investigation that could reveal a security vulnerability
- (7) **Threat Information** – Information held by the government concerning threats to any mode of transportation
- (8) **Security measures** – Access control measures; numbers and deployments of Federal Air Marshals (FAMs) and Federal Flight Deck Officers (armed pilots)



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

17

SSI Basic Training

16 SSI Categories (cont.)

- (9) **Security Screening Information** – Screening procedures for passengers and their property at the checkpoints, names on and selection criteria for the No Fly List, screen images on screening equipment, etc.
- (10) **Security Training Materials** – Records used to train screeners to perform screening functions
- (11) **Identifying Information of Certain Security Personnel** – Lists of screeners, aviation officials with airport security badges, FAMs, etc.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

18

SSI Basic Training

16 SSI Categories (cont.)

- (12) **Critical Infrastructure Asset Information** – Lists identifying systems or assets vital to the transportation system
- (13) **Systems Security Information** – Security plans for critical Federal computer/network IT systems (e.g., TSA's Secure Flight)
- (14) **Confidential Business Information** – Trade secrets required by a Security Directive



Transportation
Security
Administration

Sensitive Security Information Office
Safely Sharing Information

19

SSI Basic Training

16 SSI Categories (cont.)

- (15) **Research and Development** – Research results that were funded or directed by DHS
- (16) **Other Information** – The TSA Administrator can determine information to be SSI that is not otherwise defined in 1520.5(b)(1) – (15) *(rarely used)*



Transportation
Security
Administration

Sensitive Security Information Office
Safely Sharing Information

20

SSI Basic Training

Who is a "Covered Person"?

According to the SSI regulation, **covered persons** include airport and airline officials, maritime operators, Federal employees, contractors, and grantees, among others. Covered persons may have access to SSI.



Transportation
Security
Administration

Sensitive Security Information Office
Safely Sharing Information

21

SSI Basic Training

Persons with a "Need To Know"

Covered persons have a **"need to know"** SSI if access to information is necessary for the performance of official duties. DHS or DOT may limit access to specific SSI to certain employees or covered persons.

Example:

A screening equipment vendor does not need access to the No Fly List.



Transportation
Security
Administration

Sensitive Security Information Office
Safely Sharing Information

22

SSI and the Media



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

23

SSI Basic Training

Requests from the Media for SSI

Under the SSI regulation, members of the news media are not covered persons and do not have a "need to know" SSI.

Requests for SSI from media under state or local open records acts must be forwarded to TSA or the applicable component or agency within DHS or DOT.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

24

SSI Basic Training

Leaked SSI

Occasionally, SSI is leaked to the media.

Don't repeat leaked SSI reported in the news media or anywhere else on the Web.

In addition, unauthorized disclosure of SSI may be investigated by TSA and result in civil penalties.

Even if a major newspaper publishes SSI, it does not mean the information is no longer SSI. The SSI protection remains in effect until the TSA Administrator or his or her designee determines it is no longer SSI.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

25

Proper Marking of SSI



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

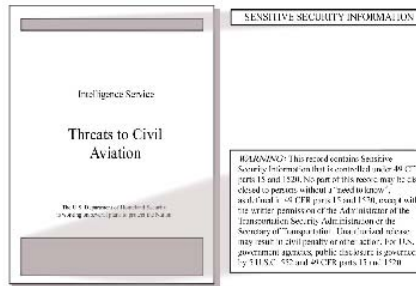
26

SSI Basic Training

SSI – Protective Marking

Any person who creates a record containing SSI must include an SSI header and footer.

Even if there is only one sentence containing SSI in a 50-page document, every page must have an SSI header and footer.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

27

SSI Basic Training

SSI Distribution Limitation Statement

The SSI footer informs the viewer that the record must be protected from unauthorized disclosure.



"WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520."



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

28

"Best Practices" for DHS Stakeholders in Protecting SSI



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

29

SSI Basic Training

What does the SSI regulation say about protecting SSI?

"Duty to protect information. A covered person must – take reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure.

When a person is not in physical possession of SSI, the person must store it in a secure container, such as a locked desk or file cabinet or in a locked room."^{*}

^{*} 49 CFR Part 1520.9(a)(1)



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

30

SSI Basic Training

When Not Under Direct Physical Control

When not actually working with an SSI record (lunch break, end of the day, etc.), store the SSI record in a locked desk drawer or in a locked room to prevent unauthorized access by persons who do not have a 'need to know.'



ALL RECIPIENTS OF SSI ARE MANDATED TO LOCK SSI UP!!!



Transportation
Security
Administration

Sensitive Security Information Office
Safely Sharing Information

31

SSI Basic Training

How has this been interpreted?

Other than locking SSI in locked drawer or cabinet, which is a requirement, **stakeholders are mandated** under the SSI regulation to take "reasonable steps" to prevent unauthorized disclosure of SSI.

The next set of slides describes "**Best Practices**" that stakeholders may use in handling and protecting SSI.

These "**Best Practices**" are based on policies and procedures developed for TSA employees to protect SSI.



Transportation
Security
Administration

Sensitive Security Information Office
Safely Sharing Information

32

SSI Basic Training

"Best Practices for Stakeholders"

SSI Transmission: E-Mail

SSI information transmitted by e-mail should be in a separate password-protected record, and not in the body of an e-mail. Passwords should be sent separately, and should:

- Be at least eight characters in length.
- Have at least one letter capitalized.
- Contain at least one number.
- Not be a word in the dictionary.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

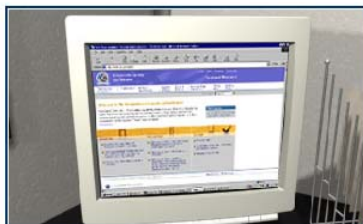
33

SSI Basic Training

"Best Practices for Stakeholders"

Web Posting SSI

TSA does NOT post SSI on its public website (i.e., Internet) or the agency-wide Intranet portal that all TSA employees and contractors have access to.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

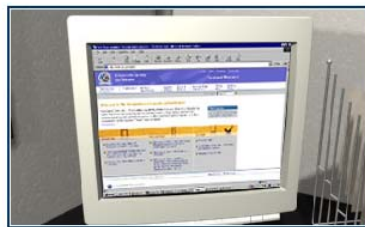
34

SSI Basic Training

"Best Practices for Stakeholders"

Web Posting SSI

TSA does NOT post SSI on its public website (i.e., Internet) or the agency-wide Intranet portal that all TSA employees and contractors have access to.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

34

SSI Basic Training

"Best Practices for Stakeholders"

SSI Transmission: Facsimile



The sender of faxed SSI should confirm that the fax number of the recipient is current and valid and the intended recipient can promptly retrieve the information.

Facsimiles sent to a controlled, secure area where unauthorized people cannot intercept the SSI material may be sent without requiring the recipient to be there.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

35

SSI Basic Training

"Best Practices for Stakeholders"

Mailing SSI

SSI may be mailed to covered persons via U.S. Postal Service (First Class only) or reliable commercial delivery services (FedEx, UPS, DHL, etc.).

When using Interoffice Mail to send SSI to covered persons, SSI should be placed in an opaque, sealed envelope.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

36

SSI Basic Training

"Best Practices for Stakeholders"

Compact Discs (CDs)

SSI stored on compact discs (CDs) should be marked with the SSI header and footer, and should be password protected.

CDs should be protected as though it were a hard-copy (paper) record (i.e., store the CD in a locked drawer.)



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

37

SSI Basic Training

"Best Practices for Stakeholders"

Flash (Thumb) Drives

Access to a portable flash drive containing any SSI should be password-protected or encrypted.

If the flash drive does not have password-protection capability or encryption, then each record stored on the drive containing SSI should be individually password-protected.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

38

SSI Basic Training

"Best Practices for Stakeholders"

Flash (Thumb) Drives (continued)

Portable drives are very convenient. They are small and can store a large volume of information. They are also easily lost or misplaced.

Please be very careful about what information is placed on the drives, how the devices are stored, and who is walking out the door with the devices.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

39

SSI Basic Training

"Best Practices for Stakeholders"

Taking SSI Home

It is not recommended!

However, if taking SSI out of the office is necessary, employees should have the permission of the supervisor and should ensure that SSI is locked away at night to prevent unauthorized access of persons who do not have a "need to know."



Transportation
Security
Administration

Sensitive Security Information Office
Safely Sharing Information

40

Destruction of SSI



Transportation
Security
Administration

Sensitive Security Information Office
Safely Sharing Information

41

SSI Basic Training

What does the SSI regulation say?

"A covered person must destroy SSI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the SSI to carry out transportation security measures."*

In other words, throwing SSI in any garbage can is not acceptable under the SSI regulation!!

* 49 CFR Part 1520.19(b)(1)



Transportation
Security
Administration

Sensitive Security Information Office
Safely Sharing Information

42

SSI Basic Training

"Best Practices of Stakeholders"

Destruction of SSI

The most common methods used to destroy SSI material include:

- Cross-cut shredders
- Cutting or tearing into pieces that are no longer than 1/2 inch on a side



Transportation
Security
Administration

Sensitive Security Information Office
Safely Sharing Information

43

SSI Basic Training

"Best Practices for Stakeholders"

DO's – SSI Safeguarding

- Do** – Lock up material containing SSI.
- Do** – Turn off or lock computer whenever left unattended.
- Do** – Properly destroy all SSI when no longer needed.
- Do** – Be conscious of surroundings when discussing SSI; remember not everyone has a "need to know" SSI.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

44

SSI Basic Training

Best Practices for Stakeholders:

DON'T's – SSI Safeguarding

- Don't** – Leave SSI unattended.
- Don't** – Discuss SSI with individuals who do not have a 'need to know.'
- Don't** – Discuss SSI on cell, wireless or cordless phones unless absolutely necessary.
- Don't** – Put SSI in the body of an e-mail.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

45

SSI Basic Training

Consequences of Unauthorized Disclosure of SSI

- Lost lives – terrorists could use the information to plan an attack.
- Lost job – for Federal employees, appropriate personnel action may be a letter of reprimand, suspension, or even dismissal and, for contractors, lost of position and access to job site.
- Lost money – the government can impose a \$10,000 civil penalty per offense on any covered person.



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

46

SSI Basic Training

Safely Sharing Information

SSI Office

Transportation Security Administration
601 S. 12th Street, East Tower, TSA-31
Arlington, VA 22202

E-Mail: SSI@dhs.gov

Phone: 571-227-3513

Fax: 571-227-2945



Transportation
Security
Administration

Sensitive Security Information Office

Safely Sharing Information

47

9 APPENDIX D: SSI GUIDANCE BROCHURE

Please refer to the Department of Homeland Security's brochure on Sensitive Security Information for additional information.

What is SSI?

Sensitive Security Information (SSI) is information that, if publicly released, would be detrimental to transportation security as defined by Federal regulation 49 C.F.R. part 1520.

Although SSI is not classified information, there are specific procedures for recognizing, marking, protecting, safely sharing, and destroying SSI.

Recognizing SSI

The following information constitutes SSI:

1. Security programs and contingency plans
2. Security directives
3. Information circulars
4. Performance specifications
5. Vulnerability assessments
6. Security inspections or investigative information
7. Threat information
8. Security measures
9. Security screening information
10. Security training materials
11. Identifying information of certain transportation security personnel
12. Critical infrastructure asset information
13. Systems security information
14. Confidential business information
15. Research and development
16. Other information as determined in writing by the TSA Administrator

The purpose of this brochure is to provide transportation security stakeholders with best practices for handling SSI. Best practices are not to be construed as legally binding requirements of, or official implementing guidance for, the SSI regulation.

The SSI Office

TSA's Sensitive Security Information (SSI) Office:

- ✓ Develops SSI guidance, policies, and procedures to help others appropriately recognize and handle SSI.
- ✓ Analyzes and reviews records for SSI content.
- ✓ Trains TSA employees, clients, and stakeholders in identifying, handling, marking, sharing, storing, transmitting, and destroying SSI.
- ✓ Coordinates with stakeholders, other governmental agencies, and Congress on SSI-related issues.

www.tsa.gov



For more information:
Phone: (571) 227-3513
Fax: (571) 227-2945
SSI@dhs.gov



Sensitive Security Information

✓ Stakeholder Best Practices Quick Reference Guide



Transportation Security Administration

Safely Sharing Information

SSI Requirements	Best Practices Guide
The SSI regulation mandates specific and general requirements for handling and protecting SSI. You Must – Lock-up All SSI When not in physical possession, store SSI in a secure container such as a locked file cabinet or drawer. You Must – When No Longer Needed, Destroy SSI Destruction of SSI must be complete to preclude recognition or reconstruction of the information. You Must – Mark SSI The regulation requires that when only a small portion of a paper document contains SSI, every page of the document must be marked with the SSI header and footer shown below. When Combining SSI With Other Sensitive But Unclassified (SBU) Information, the document must be marked as SSI. SSI extracted from SSI documents requires the new document to be marked and protected as SSI.	Reasonable Steps Must be Taken to Safeguard SSI. While the regulation does not define reasonable steps, the TSA SSI Office offers these best practices as examples of reasonable steps: ✓ Electronic Presentations (e.g., PowerPoint) should be marked with the SSI header on all pages and the SSI footer on the first and last pages of the presentation. ✓ Spreadsheets should be marked with the SSI header on every page and the SSI footer on every page or at the end of the document. ✓ Video and Audio should be marked with the SSI header and footer on the protective cover when able and the header and footer should be shown and/or read at the beginning and end of the program. ✓ CDs and DVDs should be encrypted or password-protected and the header and footer should be affixed to the CD or DVD. ✓ Portable Drives including "flash" or "thumb" drives should not themselves be marked, but the drive itself should be encrypted or all documents stored should be password-protected. ✓ When Leaving Your Computer or Desk you must lock up all SSI and should lock or turn off your computer. ✓ Taking SSI Home is not recommended, but if necessary, get permission from a supervisor and lock up all SSI at home. ✓ Discussing SSI Over Cellular Telephones should be done carefully to prevent eavesdropping. Land lines in non-public locations are more secure than cellular telephones. ✓ Email should not contain SSI in the body of the email. SSI should be emailed in a password-protected attachment. Passwords should be sent separately with no subject line or shared either in person or via telephone. ✓ Passwords for SSI Documents should contain at least 8 characters, have at least one upper-cased and one lower-cased letter, contain at least one number, and not be a word in the dictionary. ✓ Faxing of SSI should be done by first verifying the fax number and that the intended recipient will be available to retrieve the SSI once faxed. ✓ SSI Should Be Mailed by U.S. First Class mail or other traceable delivery service using an opaque envelope or wrapping and the outside wrapping should not be marked as SSI. ✓ Interoffice Mail should be sent using an unmarked, opaque, sealed envelope so that the SSI cannot be read through the envelope. ✓ SSI Stored on Network Folders should either require a password to open or the network should limit access to the folder. ✓ Destroying SSI should be done using a cross-cut shredder which produces particles that are 1½ inch by ¾ inch or smaller.
Sensitive Security Information Office	Safely Sharing Information

FOR QUESTION OR COMMENTS REGARDING THIS DOCUMENT
CONTACT THE REAL ID PROGRAM OFFICER AT (202) 447-3836 OR
VIA EMAIL AT REALID@HQ.DHS.GOV