Slide 1

Introduction, Contact Information

Welcome to the Department of General Services Information Security and Privacy Awareness training.

This training is required annually for all DGS employees / contractors and new employees upon hire.

The training is provided to you by the DGS Information Security Office (ISO).

The ISO was created to manage the development and implementation of Information Security and Privacy programs within the DGS to comply with the State Administrative Manual Sections 5300 – 5399 and Privacy.

The Information Security Office is located at the Ziggurat building in West Sacramento.

You can contact our office via email, phone or mail.

And for more information about Information Security, please visit our website at ISO.DGS.CA.GOV

Slide 2

About / Why are we here

The ISO presents the Information Security and Privacy training module to inform you about DGS and State policy.

DGS recognizes that information and department assets are essential public resources that must be protected.

Access to the information or assets is limited on a need-to-know basis only as required by law and to perform state business.

Information Security and Privacy Programs are required to protect individuals' right to privacy, department assets, and to educate staff .

Slide 3

Agenda

This presentation is part one of three presentations encompassing the entire information security and privacy training and lasts approximately 10 minutes.

In this presentation, we will introduce the Information Security Office, or ISO and give a broad overview of the subject of Information Security. We will explore department strategy, state and federal requirements regarding information security and define what the objectives of an effective security and privacy program include.

Slide 4

About the ISO

The ISO provides DGS information security and privacy oversight for compliance with State Administrative Manual and related Government Code and California Code.

It does this through:
1. Policy Development by interpreting Federal and State requirements

2. Security Awareness development for communicating policy and good security & privacy practices

3. Enterprise level Risk Management to ensure that DGS resources are protected.

4. Risk Analysis as an essential process for Divisions to ensure early detection and development of proactive protective measures.

5. Secure Business and Technology Consultation to provide divisions with guidance in the risk analysis process

6. Physical Security oversight and review.

7. Incident Management to ensure that security breaches are properly addressed and affected individuals are notified

8. Monitoring and Compliance to ensure that DGS is abiding by Federal and State requirements

Slide 5

Department Strategy

The strategic design for implementing the DGS security and privacy programs requires a team effort.

The State Administative Manual indicates that the Director is ultimately responsible for protecting of DGS assets. The ISO has delegated oversight responsibility for information security and privacy risk management. But in reality, it is a team effort which involves all DGS employees.

People are the key to making the DGS Information Security and Privacy programs a success.

All DGS Employees - Director, Executive Management, Division Management and staff are responsible for good security and privacy practices. This includes our business partners such as contractors and other state/local agencies.

By understanding how information security and privacy effects processes and technology we begin to create, use and apply good security practices. Moving forward to create a DGS security – aware culture.

Slide 6

Information Security Balancing Act

Information Security can be a balancing act between convenience and usability and good security practices.

Convenient usability is highest when security restrictions are relaxed. Heightened security while providing improved protection for assets also reduces ease of use and convenience for users.

If no security practices are in place, ease of use is extremely high and users can easily access information assets. However, in such an environment the probability of data loss or compromise is also extremely high.

Slide 7

Information Security Balancing Act

On the other end of the spectrum, if extremely rigid security measures are put in place, business processes take a back seat to security and users end up spending more time dealing with security than getting work done. In this environment security becomes an obstacle to doing business.

Slide 8

Information Security Balancing Act

Striking a balance between good security practices and acceptable levels of usability are crucial to the success of an effective information security program.

Defining information assets and determining the best approach to protect them are the first steps programs must take toward this balanced goal.

Slide 9

Requirements

The primary requirements for information security in DGS are outlined in SAM sections 5300 to 5399. These sections detail the policy that DGS must adhere to in the management of risk and protect information assets department wide.

Supporting requirements include State Constitution Article 1 protecting an Individual's Right to Privacy.

Government Code Sections 6250-6265 and the California Public Records Act provide for the inspection of public records.

Civil Code Section 1798 and the Information Practices Act (IPA) of 1977 detail specific requirements to State collection, use, maintenance and dissemination of private information.

Government code Sections 14740-14770 and State Administrative Manual 1601-1699. address the creation, use, maintenance, retention, preservation and disposal of state records.

Computer Data Access and Fraud Act (Penal Code Section 502) ensure protection from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. It allows for civil action against any person convicted of violating the criminal provisions for compensatory damages

Technology and business process advances in the digital world have increased the risk to information and continue to impact the development and updates to laws that protect security and privacy.

More information on each of these laws and policies is available at the ISO web site, or call our office if you have questions.

Slide 10

Security And Privacy Objectives

The key function for Information Security and Privacy programs within DGS is to ensure that DGS's information assets are protected.

In order for DGS to successfully accomplish its mission and each Division to conduct their job functions in support of that mission, we depend on our assets or resources to be reliable, accessible and available when we need them.

- Confidentiality – collection, access, and disclosure
- Integrity – accuracy and consistency
- Availability – timely accessibility to the resources

Protection of department assets is accomplished through risk management functions.
The first step being risk analysis which helps identify the assets, the threats and specific methods to protect them.

Slide 11

Confidentiality

Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems.

For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant for processing. The system attempts to enforce confidentiality by encrypting the card number during transmission and by restricting access to the places where it is stored or displayed. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information.

Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a business holds

Slide 12

Integrity

Information integrity means that data cannot be modified without authorization.

Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on.

There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could mis-type someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised.

Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.

Slide 13

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.

Availability is threatened by unauthorized access or intentional interruption to information or systems.

Examples of availability interruptions are lost or stolen documents, unsecured web applications (web pages) or data bases, unstable or unreliable connection to the network, systems, email, or other services.