Security Overview

Secure E-Mail

Internet/E-mail Security Alerts

Security Overview

Home | A&E | O&R | PDR | P&A | R&C | M&O

Information Security Overview

The FDA Information Security program, under the direction of the Chief Information Security Officer (CISO) Joe Albaugh, consists of several focal areas whose objectives are to keep FDA intellectual and physical property safe and secure by adding security layers, monitoring systems and resources, pro-actively defending against threats, aligning business and information security policies, and dealing with incidents.

Throughout these pages, we will identify each focal area in greater detail. You will be able to read a description of each focal area as it relates to our purposes at FDA, identify contacts, and gain access to the resources provided by each area [if applicable].

FDA Information Security Focal Areas

- Architecture & Engineering [**A&E**]
- Operations & Response [**O&R**]
- Planning & Disaster Recovery [**PDR**]
- Policy & Awareness [**P&A**]
- Risk & Compliance [**R&C**]
- Management & Oversight [**M&O**]

Alert Notification

The Information Security team has received reports of a phishing email with the sender claiming to be the Federal Bureau of Investigations (FBI). This email is a hoax and an attempt to gain access to your personal information. (Copy of the Email)

Phishing, a form of social engineering, is becoming an increasing problem. For details on how to handle these emails and any similar phishing emails, please check out the content on Phishing in the new Mastering Cyber Security section: Phishing & Social Engineering

Security Overview

- Secure E-Mail
- Internet/E-mail Security Alerts

Operations & Response (O&R)

Home | A&E | O&R | PDR | P&A | R&C | M&O

Operations & Response

The Operations & Response (O&R) focal area consists of the Security Operations Center (SOC) and the Incident Response (IR) staff.

O&R Summary	
Building:	OAK 8
Center:	OC
Organization:	Division of Technology
Branch:	Security
FDA Lead:	Scott Spitnale

The SOC and IR are part of the consolidated FDA Security program and overall security operations of the FDA. A portion of the mission and purpose of the SOC and IR is to assist in the reduction of risk, and having a dynamic view of the traffic and "events" that take place in the FDA computing environment. Currently, the IR SOC activities include vulnerability scanning of FDA systems, validating patch levels, configuration hardening, WEB monitoring/site blocking, and other system safeguards.

The FDA SOC and IR utilizes a set of tools that view events, correlate events that have known malicious signatures, or anomalous characteristics, and intervene when traffic or events suggest that some violation or malicious activity is taking place in the FDA network environment. When a problem is suspected, various tools and mechanisms can be used to forensically analyze event history and associated activity, and the cause can be identified to a point in time and often to a source location.

Security Overview

Secure E-Mail

Internet/E-mail Security Alerts

Planning & Disaster Recovery (PDR)

Home | A&E | O&R | PDR | P&A | R&C | M&O

PDR Description | FDA Alert System (FDA AS)

Planning & Disaster Recovery

The Planning and Disaster Recovery focal area supports Information Technology by developing and maintaining the Continuity of Operations Plan Strategies which support the FDA's eight Mission Essential Functions.

Specifically, the PDR focuses on how to prepare, prevent, respond, and recover from a prolonged disruption. The objectives are to keep the organization operating during and after a disruption. Types of disruption include natural disasters; people (in the form of sabotage, hacking, terrorism, etc.); or technical events such as computer virus or power failure.

PDR Summary

Building:	OAK 8
Center:	OC
Organization:	Division of Technology
Branch:	Security
FDA Lead:	Stefan Trach
Contact:	FDA-PDRT@fda.hhs.gov

The goal of the PDR focal area is to formulate a Disaster Recovery Plan. The plan attempts to capture, in detail, how FDA will respond, recover, and reconstitute its IT following a disruption. These plans address the initial actions (response), crisis management, interruption resolution (recovery), and return to normal operations (reconstitution). In addition, the Disaster Recovery Plan will document the IT resource requirements, and procedures to follow for successful recovery of the Primary and Secondary Mission Essential Functions.

Continuity Strategies

- IT Disaster Recovery events
- Pandemic Influenza events
- Counter Terrorism events
- Critical Infrastructure Protection system threats

Primary Mission Essential Functions

1. Provide agency leadership and program coordination.
2. Ensure the availability and safe use of medical products.
3. Communications and Response -- Coordinate domestic and international communications and response activities related to emergencies that impact the safety, efficacy, integrity or availability of FDA-regulated products or that require FDA's investigational or laboratory support to other government agencies.
4. Provide expert analysis and advice regarding radiological health (electronic product, radiation exposure, radioactive contamination of food and medical products, etc.)
5. Ensure the safety and integrity of the blood supply.
6. Ensure the safety and integrity of the supply chain for all FDA-regulated products (human and animal food, human and animal drugs, medical devices, biologics, radiological products, cosmetics).
7. Ensure the integrity of the import safety system.
8. Monitor and respond to adverse event incidents and consumer complaints.

Security Overview

- Secure E-Mail
- Internet/E-mail Security Alerts

Policy & Awareness (P&A)

Home | A&E | O&R | PDR | P&A | R&C | M&O

Training | FDA IT Security Policies | Online Security Awareness Course

Policy & Awareness

The purpose of the Policy & Awareness focal area is to provide FDA users with a successful awareness program through various channels such as IT security policy and security awareness tools, resources and IT Security training.

P&A Summary	
Building:	OAK 8
Center:	OC
Organization:	Division of Technology
Branch:	Security
FDA Lead:	Maureen Moore
Contact:	FDA IT Security Policy

Policy

This part of the focal area is responsible for the development and revision of FDA IT Security policies (3250 series). Team members oversee the policy review and approval process through to its publication. Once the current state of revising all policies is complete, all IT security policies will be reviewed on an annual basis.

Security Awareness

This part of the focal area is responsible for providing users with security awareness through several channels including the Online Security Awareness Course, briefings, events, newsletters, communications, and the Information Security website.

Training

This part of the focal area is responsible for developing and implementing role-based training to users with significant security responsibilities, as well as ensuring the internal Information Security team is properly trained to support the CISO and FDA in the area of information security.

The IT Defender

- Phishing
- FDA's Alert System
- Celebration of Cyber Security Awareness Month
- How to Report an Incident

Mastering Cyber Security

"Mastering Cyber Security" seeks to impart knowledge about protecting that information by detailing ways to prevent, detect, and respond to the various forms of attacks that are utilized today.

Cyber Security HOT Topic
Phishing & Social Engineering

What is phishing and how can you protect yourself from phishing attacks?

Mastering Cyber Security | The List | General Protection Tips

Security Overview

- Secure E-Mail
- Internet/E-mail Security Alerts

Mastering Cyber Security: Phishing

Home | A&E | O&R | PDR | P&A | R&C | M&O

Training | FDA IT Security Policies | Online Security Awareness Course

The List

Mastering Cyber Security * The List * General Protection Tips

Phishing & Social Engineering

Phishing

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as:

- natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
- epidemics and health scares (e.g., H1N1)
- economic concerns (e.g., IRS scams)
- major political elections
- holidays

Social Engineering

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

Security Overview

Secure E-Mail

Internet/E-mail Security Alerts

Risk & Compliance (R&C)

Home | A&E | O&R | PDR | P&A | R&C | M&O

NIST Resources

Risk & Compliance

The Risk and Compliance (R&C) focal area ensures compliance with FISMA, OMB, HHS, and FDA mandates. They are responsible for assisting System Owners and Business Owners with the Security Authorization Process of their information systems. R&C validates that all Management, Operational and Technical controls across the agency are implemented correctly, operating as intended and producing the desired results according to NIST and HHS guidance.

For questions/requests/information on Security Authorization, please contact FDASecurityAuthorization@fda.hhs.gov

R&C Summary	
Building:	OAK 8
Center:	OC
Organization:	Division of Technology
Branch:	Security
FDA Lead:	Nipa Shah

***Security Authorization Toolkit**: This toolkit will provide answers to questions about Security Authorizations. For instance, why FDA needs Security Authorizations, what are the roles, and where to find the Security Authorization Policy.*

Communications & Resources

- Accounts and Passwords
- All Hands Announcements
- IT Defender
- IT Security News

Communications & Resources

Home | Accounts & Passwords | IT Defender | All Hands Announcements | IT Security News

Configuration Standards | Contracts/SOW Requirements | Processes and Procedures

Reveal this week's Information Security Tip

Communicating and providing individuals with the resources empowering them to "be secure" is an essential component of an effective information security program. This section will help keep you in the know and assist you with understanding your part to contributing and maintaining a united front against information security threats affecting the FDA and you.

In this section, you will find:

- Accounts and Passwords - An informational resources for passwords policies, new account requests and password resets.
- IT Defender - A quarterly security awareness newsletter with information such as articles on current security threats, helpful tips and reminders, etc.
- All Hands Announcements - Key announcements published by the Office of Information Management (OIM)
- IT Security News - A sample of external resources on and about information and technology security.
- Configuration Standards - Information Security System Configuration Standards.
- Contracts/SOW Requirements - Information Security Requirements for Contracts and Statements of Work.
- Processes and Procedures - Step by step documents to assist FDA employees in achieving the goals related to their tasks.

IT Security is a growing and constantly evolving arena; new and changing threats from inside and outside the organization are abundant. Therefore it is critical that each of us are aware of, understand , and practice IT Security in all we do.

Check back here often as we continually update this section so that you can, **"Be Secure!"**

Communications & Resources

- Accounts and Passwords
- All Hands Announcements
- IT Defender
- IT Security News

All Hands Announcements

Home | Accounts & Passwords | IT Defender | All Hands Announcements | IT Security News

All Hands Announcements

In the related links below, you will find copies of recent announcements from the OIM in regards to Information Security; check back as we continuously add new announcements.

Related inside.FDA Links

- IT Defender Issue 3 Announcement
- OIM New Content on the Information Security Website
- Security Notification - Safeguarding of Classified Information
- Alert Notification - Recent Increase in FBI Phishing Emails to FDA Community

If you would like to view previous announcements, you can visit the All Hands Announcements Archives.

Stay informed on IT Security topics and find out about current events, by checking out the latest issue of:

IT Defender From the OIM Information Security Program

February 2011 Issue 3

FAQs

- Firewall
- Planning & Disaster Recovery
- Policy & Awareness
- Remote Access
- Risk & Compliance
- Security Operations Center

Risk & Compliance

Home | Firewall | PDR | P&A | Remote Access | R&C | SOC

I. Security Authorization

a. Where can I find information on the Security Authorization process such as what systems require authorization, what the current policy is, etc?

II. Audits

a. I received an audit request, what do I need to do?

I. Security Authorization

a. Where can I find information on the Security Authorization process such as what systems require authorization, what the current policy is, etc?

Check out the Security Authorization Toolkit for more information on the security authorization process. If the toolkit does not answer your question, please contact:

FDASecurityAuthorization@fda.hhs.gov

Back to FAQ list

II. Audits

a. I received an audit request, what do I need to do?

IT Security audits are considered extremely important and both compliance with audit requests and final audi findings are monitored by FDA senior management.

- Open all messages concerning audits immediately.
- Determine if you are the person to supply the information.
  - If you are not the correct POC, Reply to All and, if possible, indicate who the POC is.
  - If you are the correct POC, Reply to All that you've received the message and acknowledge that you will return the items requested prior to the due date.
- Read the request carefully. If you do not understand the request, Reply to All and ask for clarification.
- Provide exactly what was requested and no more than what was requested prior to the due date. All material provided must be in final (not draft) form and must be presented professionally.
- Be prepared for follow up requests from the auditors.

FDA usually has a very short period of time in which to respond to requests for information from the auditors. Your prompt and thoughtful response to all requests will allow FDA to meet deadlines and reduce the numbe of follow up requests.

Back to FAQ list

The IT Security section of FDA's intranet is a place where employees can keep informed about the latest news on FDA IT Security and how to help keep information secure. The website is grouped into four sections: Security Overview, Communication & Resources, Training, and Frequently Asked Questions.

•**The Security Overview section** describes the FDA Information Security program, consisting of several focal areas whose objectives are to keep FDA intellectual and physical property safe and secure. These pages provide a detailed description of each focal area as it relates to our purposes at FDA, identifies contacts, and how to gain access to the resources provided by each area [if applicable]. FDA Information Security Focal Areas include:

- Architecture & Engineering [A&E],
- Operations & Response [O&R],
- Planning & Disaster Recovery [PDR],
- Policy & Awareness [P&A],
- Risk & Compliance [R&C],
- Management & Oversight [M&O] (which includes Accounts Audit Management and Information System Security Officers)

•**The Communication & Resources section** keeps employees in the know and assists with understanding their role in contributing and maintaining a united front against information security threats affecting the FDA and it's employees. The resources in this section include:

IT Defender - A quarterly security awareness newsletter with information such as articles on current security threats, helpful tips and reminders, etc. All Hands Announcements - Key announcements published by the Office of Information Management (OIM).
IT Security News - A sample of external resources on and about information technology security.
Configuration Standards – Links to Info System Security Configuration Guides
Contracts/SOW Requirements - Information Security Requirements for Contracts and Statements of Work.
Processes and Procedures - Step by step documents to assist FDA employees in achieving the goals related to their tasks.

•**The Training section** links employees to all of the necessary resources for staying compliant and up to date on the latest available training in the area of IT security.

•**The Frequently Asked Questions section** provides a place for employees to look for answers to common questions and issues related to Information Security.