Information Security
Monthly Activity Report*

INFOCON LEVEL
CRITICAL
SEVERE
ELEVATED
GUARDED
NORMAL

August 2015

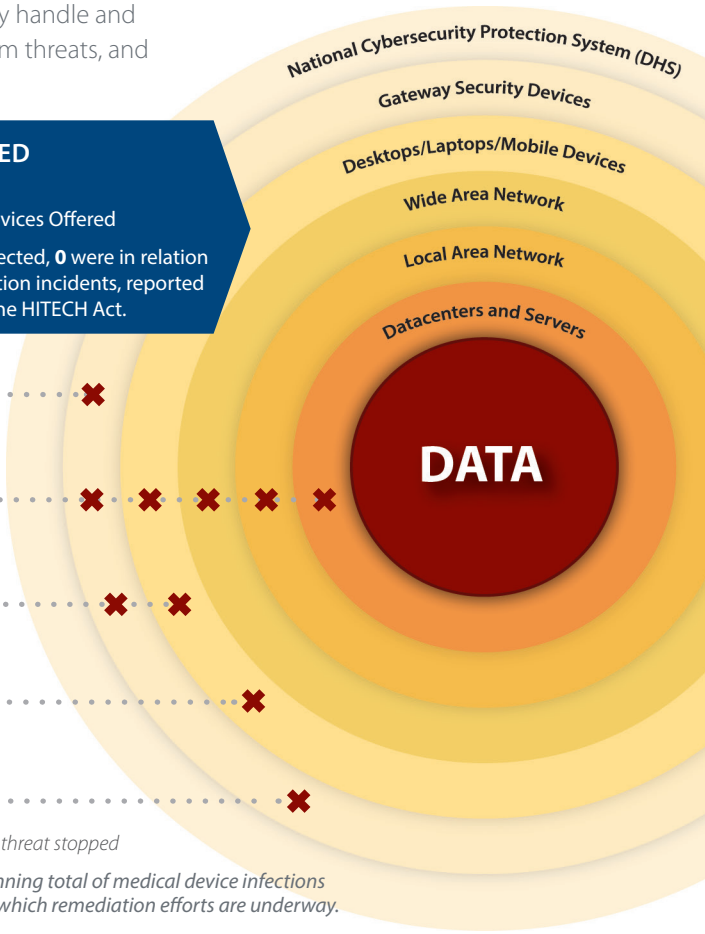
VA uses a defense-in-depth approach to information security to protect the data we hold on Veterans. While the defense-in-depth approach protects from inbound threats and contains other data exposing incidents, VA relies on employees to protect Veteran information they handle and transmit. This graphic demonstrates how the layered defense protects Veterans from threats, and where data exposures have occurred for the past month.

Threats Blocked or Contained By VA's Defense In Depth

0 VETERANS AFFECTED

- **0** Notifications
- **0** Credit Protection Services Offered

Of the total # of Veterans affected, **0** were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



Intrusion Attempts (Blocked)
235,211,165

Malware (Blocked/Contained)
587,790,803

Suspicious/Malicious Emails (Blocked)
98,628,159

Infected Medical Devices (Contained)**
3

Outgoing Unencrypted Emails
72 Associated Privacy/Security Events
15,694 Total Emails Blocked

✖ = *threat stopped*

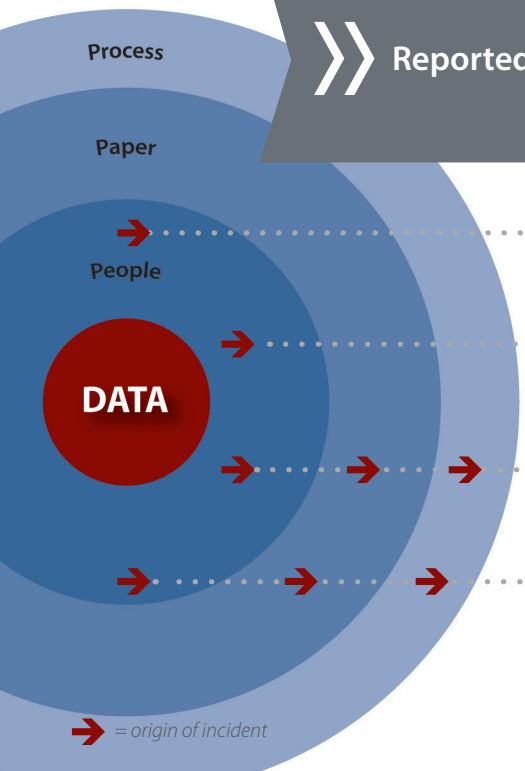
** *Running total of medical device infections for which remediation efforts are underway.*

Reported Events

431 VETERANS AFFECTED

- **127** Notifications
- **304** Credit Protection Services Offered

Of the total # of Veterans affected, **237** were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



→ = *origin of incident*

Lost and Stolen Device Incidents
47

Lost PIV Cards
117

Mishandled Incidents
84

Mis-mailed Incidents
148 Paper Mis-mailings
1 Pharmacy-item Mis-mailings
out of **6,811,826** Total Mailings

* This graphic is a visual depiction of VA's information security defense in depth. It is not intended to provide an exhaustive summary of VA's information security activity. This data, which is extracted from Data Breach Core Team and US-CERT reporting, represents a snapshot in time and is subject to change based on further validation.

DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Incident Resolution Service

Monthly Report to Congress of Data Incidents

August 1-31, 2015

Security Privacy Ticket Number:	PSETS0000123182
DBCT Category:	IT Equipment Inventory
Organization:	VISN 05 Baltimore, MD
Date Opened:	8/10/2015
Date Closed:	8/18/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0624466
Date US-CERT Notified:	8/10/2015
US-CERT Case Number:	INC000010020150
US-CERT Category:	Category 1 - Unauthorized Access
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

During an Information Resources Management (IRM) Service Delivery and Engineering (SDE) wall to wall inventory, IT equipment was discovered missing and was reported to the Information Security Officer (ISO). The Chief Information Officer (CIO) is working with the facility Police Service, Acquisition, and leadership to address the loss.

Incident Update

On August 10, 2015 the following 49 items were originally determined to be missing:
2 - Laptops
7 - Servers
3 - Workstations
2 - Tablets
12 - Network Switches
23 -Other miscellaneous equipment such as printers, scanners, and monitors.

On August 18, 2015 the Acting CIO provided an update stating that upon further investigation the original list of items missing had been reduced to 29 with the estimated value having been reduced from $190,000 to $42,900.

The Incident Resolution Service Team has determined that no data breach has occurred.

Resolution

Facility staff has been instructed to maintain more accurate inventory records, and ensure that all personally assigned items are properly safeguarded from loss.

DBCT

This incident was discussed by the DBCT, but no DBCT decision is required. This is informational for IT Equipment Inventory incidents and is the representative ticket. There was only one IT Equipment Inventory Incident this reporting period.

Security Privacy Ticket Number:	PSETS0000123483
DBCT Category:	CMOP Mismailed
Organization:	VHA CMOP Hines, IL
Date Opened:	8/17/2015
Date Closed:	9/3/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0624749
Date US-CERT Notified:	8/17/2015
US-CERT Case Number:	INC000010021923
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	
No. of Loss Notifications:	1

Incident Summary

Patient A received a Medline Industries medical supply intended for Patient B. Patient B's name and type of medical supply was compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. Great Lakes Consolidated Mail Outpatient Pharmacy (CMOP) investigation concluded that this was a Medline packing error. The packing error has been reported to Medline for investigation and corrective action.

Incident Update

08/17/15:
The Incident Resolution Service Team has determined that Patient B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

On August 17, 2015 the packing error was reported to Medline for investigation and corrective action.

DBCT

No DBCT decision is required. This is informational for Mis-Mailed CMOP incidents and is the representative ticket. There was only one Mis-Mailed CMOP incident out of 6,811,826 total packages (9,747,544 total prescriptions) mailed out for this reporting period. In this incident, the affected individual will receive a HIPAA notification letter.

Security Privacy Ticket Number:	PSETS0000123527
DBCT Category:	Mismailed
Organization:	VBA Indianapolis, IN
Date Opened:	8/18/2015
Date Closed:	8/24/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0624794
Date US-CERT Notified:	8/18/2015
US-CERT Case Number:	INC000010022295
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	1
No. of Loss Notifications:	

Incident Summary

A letter received by Veteran A contained Veteran B's name, address, and SSN which Veteran A provided to his Veteran Service Officer (VSO), who then returned it to VA.

Incident Update

08/18/15:
The Incident Resolution Service Team has determined that Veteran B will be sent a letter offering credit protection services due to full SSN being disclosed.

Resolution

The responsible employee was counseled by his supervisor on August 21, 2015.

DBCT

No DBCT decision is required. This is informational for Mis-Mailed incidents and is the representative ticket. There were a total of 148 Mis-Mailed incidents this reporting period. Because of repetition, the other 147 are not included in this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Security Privacy Ticket Number:	PSETS0000123537
DBCT Category:	Mishandling
Organization:	VISN 04 Wilkes-Barre, PA
Date Opened:	8/18/2015
Date Closed:	9/2/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0624929
Date US-CERT Notified:	8/21/2015
US-CERT Case Number:	INC000010023372
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	
No. of Loss Notifications:	1

Incident Summary

Veteran A was provided a copy of Veteran B's appointment list when he was discharged from the ICU. It was determined that Veteran B's appointment list was mistakenly attached to Veteran A's appointment list.

Incident Update

08/21/15:
The Incident Resolution Service Team has determined that Veteran B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

Veteran A returned the appointment list that belonged to Veteran B and the Service Chief has been contacted to determine the underlying cause and ensure actions are taken to prevent future incidents.

DBCT

No DBCT decision is required. This is informational for Mis-Handling incidents and is the representative ticket. There were a total of 84 Mis-Handling incidents this reporting period. Because of repetition, the other 83 are not included in this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.