Department of Veterans Affairs **VA Handbook 6500.2**
Washington, DC 20420 **Transmittal Sheet**
June 17, 2008

MANAGEMENT OF SECURITY AND PRIVACY INCIDENTS

1. REASON FOR ISSUE: This establishes procedures for Department of Veteran Affairs (VA) management of incidents involving VA sensitive information and/or information systems, and implements the policies set forth in Veterans Affairs (VA) Directive and Handbook 6500, *Information Security Program*; the Federal Information Security Management Act of 2002 (FISMA), Pub. L. No. 107-347, 116 Stat. 2946, codified at 44 U.S.C. §§ 3541-3549; Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection (Dec 17, 2003); Department of Veterans Affairs Information Security Enhancement Act of 2006, Pub. L. No. 109-461, 120 Stat. 3450, codified at 38 U.S.C. §§ 5721-28; and Information Security matters, 38 C.F.R. §§ 75.111-119.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: In accordance with the provisions of VA Directive 6500, *Information Security Program*, and in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-61, *Computer Security Incident Handling Guide*, this Handbook outlines the procedures required to initiate, coordinate, and manage security and privacy incidents within VA.

3. RESPONSIBLE OFFICE: The Office of the Assistant Secretary for Information and Technology (OI&T) (005R3).

4. RELATED DIRECTIVE: VA Directive 6500, Information Security Program and VA Handbook 6500, Information Security Program Handbook.

RESCISSIONS: None

CERTIFIED BY:	**BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS**
/s/ Robert T. Howard Assistant Secretary of Information and Technology	**/s/** Robert T. Howard Assistant Secretary of Information and Technology

Distribution: Electronic Only

MANAGEMENT OF SECURITY AND PRIVACY INCIDENTS

TABLE OF CONTENTS

TOPIC **PAGE**

MANAGEMENT OF SECURITY AND PRIVACY INCIDENTS

1. PURPOSE AND SCOPE

a. This Handbook provides incident response guidance to ensure appropriate and expeditious handling of incidents involving the security and privacy of VA sensitive information or information systems that may adversely affect VA's normal business operations. The procedures in this Handbook address the roles and responsibilities of the VA Network and Security Operations Center (NSOC), the Incident Resolution Core Team (IRCT), Chief Information Officers (CIO), Privacy Officers (PO), Information Security Officers (ISO), and users. It provides a general overview of the incident handling process that includes:

(1) end user detection of the security/privacy event;

(2) end user reporting of the event to his/her supervisor, ISO, and/or Privacy Officer (PO);

(3) steps the ISO and/or PO take;

(4) procedures that the VA Network and Security Operations Center (VA-NSOC) and the VA Incident Resolution Core Team (VA IRCT) follow to mediate and provide guidance to the field;

(5) management for Department of Veterans Affairs in monitoring, reporting and providing guidance/procedures to the field in alleviating future events.

b. The procedures in this Handbook apply to the following:

(1) All VA employees, contractors, researchers, students, volunteers, representatives of Federal, State, local, or Tribal agencies, and all others authorized access to VA facilities, information systems or information in order to perform a VA authorized activity.

(2) All received information both in electronic and hard copy form that is created, collected, processed, transmitted, stored, or disseminated using a VA information system.

(3) VA or contractor-operated services and information resources located and operated at contract facilities, at other government agencies that support VA mission requirements, or at any other third party site utilizing VA information in order to perform a VA authorized activity. External organizations are also subject to any Data Transfer Agreements, Memoranda of Understanding, Memorandum of Agreements, or Business Associates Agreements that are developed to protect the security and integrity of VA sensitive information that they are handling

2. BACKGROUND

a. The Office of Management and Budget (OMB) Circular A-130 Nov. 30, 2000 requires VA to ensure that there is a capability to help users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability shall share information with other organizations and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance.

b. Department of Veterans Affairs Information Security Enhancement Act of 2006, Pub. L. No. 109-461, 120 Stat. 3450, codified at 38 U.S.C. §§ 5721-28, established information technology security requirements for Sensitive Personal Information that apply to the Department of Veterans Affairs. The act mandates, among other things, that VA develop procedures for detecting, immediately reporting, and responding to security incidents; notify Congress of any significant data breaches involving sensitive personal information; and, if necessary, provide credit protection services to those individuals whose sensitive personal information has been compromised.

c. The Federal Information Security Management Act of 2002 (FISMA) requires agencies to have procedures in place for detecting, reporting, and responding to security incidents. An incident, as it relates to this handbook, is defined as any event that has resulted in: unauthorized access to, or disclosure of, VA sensitive information; unauthorized modification or destruction of system data, reduced, interrupted, or terminated data processing capability; introduction of malicious programs or virus activity; or the degradation or loss of the systems confidentiality, integrity, or availability; or the loss, theft, damage, or destruction of any equipment containing VA data.

d. Incidents pose a threat to the confidentiality, integrity, availability, or privacy of data or systems. They may result in a failure of security controls; an attempted, suspected, or actual compromise of information; or the waste, fraud, abuse, loss, or damage of government property or proprietary information. The term "incident" encompasses the following general categories of adverse events:

(1) Disruption of service. Users rely on services provided by network and computing services. Perpetrators and malicious code can disrupt these services in many ways, including: erasing a critical program, "mail spamming" (flooding a user account with e-mail), and altering system functionality by installing a Trojan horse program

(2) Hoaxes occur when false information about incidents or vulnerabilities is spread.

(3) Malicious code attacks include attacks by programs such as viruses, Trojan horse programs, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Malicious code is particularly troublesome in that it is written to masquerade its presence and, thus, is often difficult to detect. Self-replicating malicious code such as viruses and worms can furthermore replicate rapidly, thereby making containment an especially difficult problem.

(4) Misuse occurs when someone uses a computing system for something other than official or VA approved purposes.

(5) Unauthorized access occurs when an individual gains logical or physical access without permission to a Federal agency network, system, application, data, or other resource. This encompasses a range of incidents from improperly logging into a user's account (for example the use of someone else’s codes to log in to a VA resource) to unauthorized access to files and directories stored on a system or storage media. Unauthorized access could also entail access to network data by using an unauthorized program or device to capture data traversing the VA network.

(6) Privacy Breach. The loss, theft, or any other unauthorized access, other than those incidental to the scope of employment, to data containing Sensitive Personal Information (SPI) in electronic, printed, or any other format, results in the potential compromise of the confidentially or integrity of the data regardless of the manner in which the breach might have occurred.

e. The primary goal of incident management is to restore normal service operations as quickly as possible and minimize the adverse impact on mission operations, thus ensuring that acceptable levels of confidentiality, integrity, and availability are maintained. Incident management is a critical process that provides the ability to detect incidents, diagnose the problem and then mitigate the problem quickly and efficiently.

f. The process also provides management with accurate and timely information on the incidents as it relates to the impact on business operations to mitigate the problem. By utilizing an incident management process, VA can ensure that support resources are focusing on the issues that have the greatest urgency and potentially the greatest impact.

g. The objectives of incident management are as follows:

(1) To restore normal services as quickly as possible

(2) To minimize the impact of incidents on VA operations.

(3) To ensure that incidents are processed consistently and are reported to show accountability.

(4) To handle all detected incidents through the VANSOC.

(5) To provide information in the form of guidance and/or lessons learned that reduces the number of incidents and allows management planning to be carried out in the most effective manner

(6) To detect, contain and prevent the spread of viruses

(7) To direct support resources appropriately

h. Key benefits of incident management are:

(1) Timely resolution of incidents, resulting in minimized impact of the disruption

(2) Improved utilization of support resources

(3) Better understanding of the impact of incidents allowing improved prioritization

(4) Accurate information on the incidents as they occur

(5) Increased availability of management information

(6) Improved confidentiality, availability and the integrity of information processing systems throughout VA

(7) Effective risk mitigation through incident resolution and taking corrective actions to prevent recurrence.

i. The purpose of specifying incident response policy and procedures includes:

(1) Helping personnel quickly recognize, identify and efficiently recover from security incidents

(2) Minimizing loss or theft of information, and the disruption of critical computing services when incidents occur

(3) Providing a means to respond systematically. Following procedures increases the likelihood that personnel will carry out all necessary steps to correctly handle an incident.

(4) Protecting the confidentiality, integrity, and availability of information. Being able to quickly detect and recover from incidents is a protection strategy that supplements system and network protection measures

(5) Protecting personnel. Many VA personnel and veterans depend on computing systems to protect their privacy and ensure their safety as it relates to health care delivery. . Following sound incident response procedures minimizes the likelihood that these systems will function improperly or will become inoperable after a security incident occurs

(6) Using resources efficiently. Having management, technical and operational personnel respond to an incident requires a substantial amount of resources. These resources could be devoted to another mission if an incident were to be short lived. Ending the incident as quickly as possible is, therefore, a high priority so that resources can once again be expended on "normal" operations.

3. DOCUMENT STRUCTURE: This Handbook is comprised of four main sections that make up the VA incident response process, based on the procedures outlined in NIST Special Publication 800-61(see Figure 3-A, below). The roles and responsibilities of VA's incident response teams are outlined under each of these categories. Appendices have been provided to further clarify information contained in some of the sections. The four sections of this handbook are: (Description of Figure 3-A)

(1) Preparation

(2) Detection, Reporting, and Analysis

(3) Containment, Eradication, and Recovery

(4) Post-incident Activity

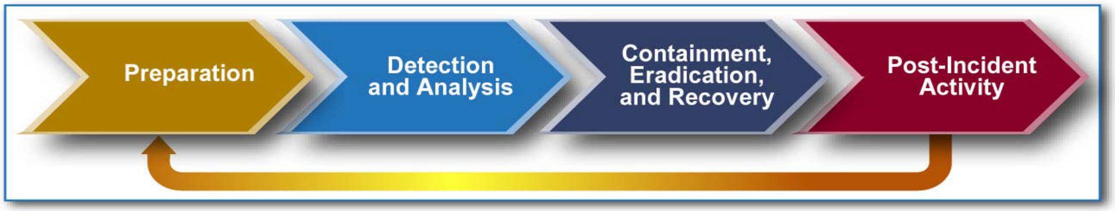


Figure 3-A. VA Incident Management Process

4. PREPARATION

a. How well VA prepares in advance for detecting and handling privacy and security incidents will greatly affect how well the users of VA information and information systems will respond when an incident is detected. During preparation, VA will select and implement security controls for its information systems in accordance with established policy and based on the results of risk assessments performed at the national and local level. Implemented security controls will be documented, as well as any residual risk to the information systems. System owners are responsible for taking appropriate actions towards mitigating and reducing residual risk.

b. Per the OMB Memorandum dated September 20, 2006, titled “Recommendations for Identity Theft Related Data Breach Notification,” VA established an Incident Resolution Team Structure (IRTS) for data breach mitigation -- a response structure that includes a core upper management level group from the local, regional/district and national levels. This VA-wide organization evaluates and handles incidents where data confidentiality has been breached and sensitive personal information (SPI) may have been exposed to identity theft. It should be viewed as a matrix structure from the local to the national level that operates both vertically and horizontally.

c. OMB recommends in its memorandum that all agencies establish such a group to handle data breaches that may result or have resulted in the misuse of SPI, or that show evidence of identity theft. Preparation for and responding to a major loss of sensitive personal information is a complex task and requires the cooperative efforts of many VA offices , in partnership with the functional areas supporting the "business" lines within VA. The IRTS role is to employ the necessary assets within the structure to assess the impact, mitigate any possible harm, take corrective action, and normalize operations to protect the individual(s) whose confidential records may have been exposed or compromised.

Figure_4A.htm (Select this link for a text description of Figure 4-A)

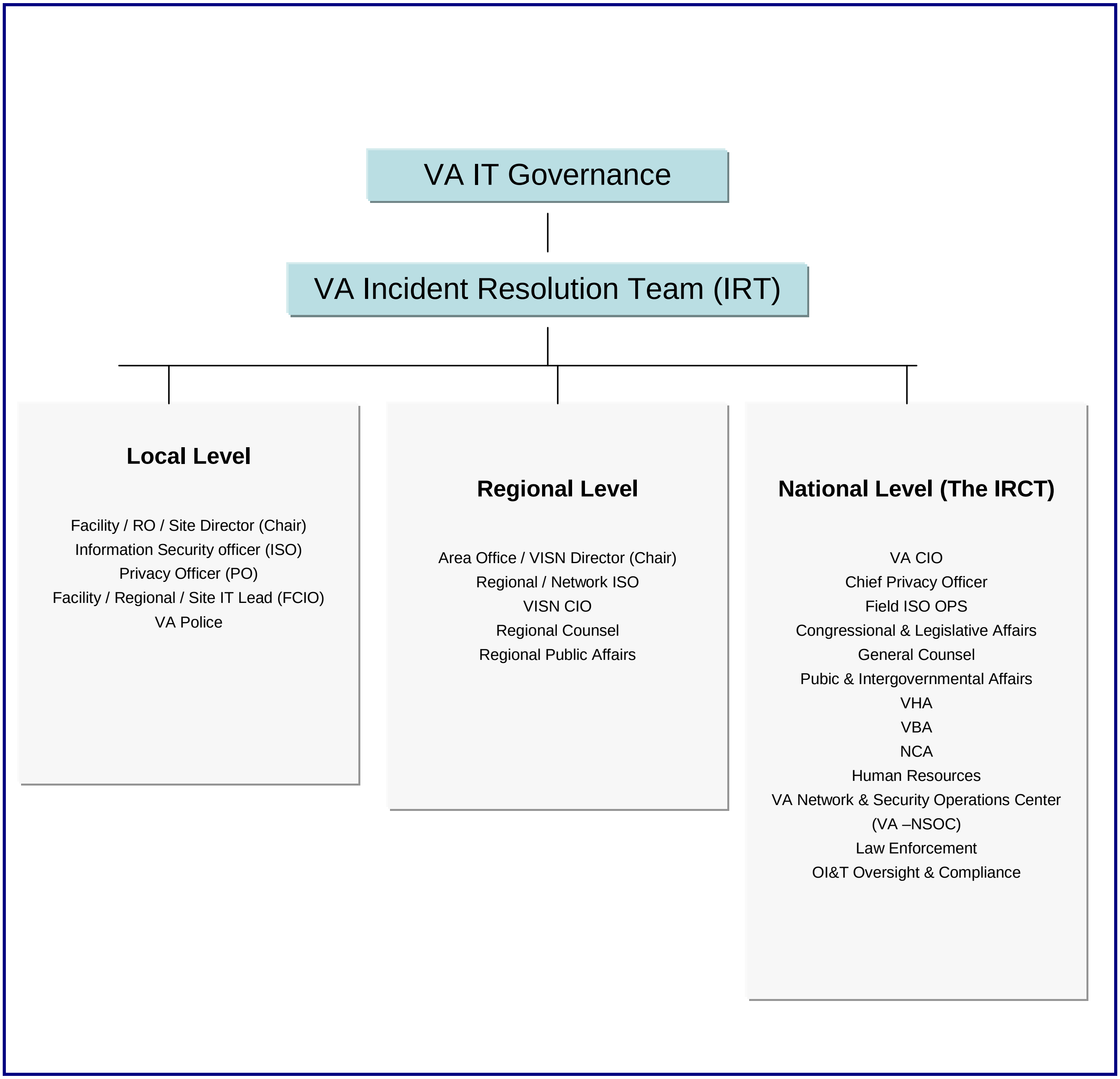

VA IT Governance
VA Incident Resolution Team (IRT)
Local Level
Facility / RO / Site Director (Chair)
Information Security officer (ISO)
Privacy Officer (PO)
Facility / Regional / Site IT Lead (FCIO)
VA Police
Regional Level
Area Office / VISN Director (Chair)
Regional / Network ISO
VISN CIO
Regional Counsel
Regional Public Affairs
National Level (The IRCT)
VA CIO
Chief Privacy Officer
Field ISO OPS
Congressional & Legislative Affairs
General Counsel
Pubic & Intergovernmental Affairs
VHA
VBA
NCA
Human Resources
VA Network & Security Operations Center
(VA –NSOC)
Law Enforcement
OI&T Oversight & Compliance

Figure 4-A. VA Incident Resolution Team Structure

d. Assignments are made by the Incident Resolution Team (IRT) levels for developing appropriate procedures and actions related to incident response. Incident Resolution organizations at each level may appoint temporary project working groups to address SPI data issues within their areas of responsibility.

(1) Roles. Specific roles and responsibilities within the IRTS (see Figure 4-a) include:

(a) The National VA Incident Response Core Team (IRCT) provides oversight and monitors the data breach incident resolution process and ensures that appropriate actions are taken in a timely manner, and that appropriate reports and notifications are drafted for VA officials and Congress.

(1) Coordinates a risk-based response to information security or privacy incidents at the national level.

(2) Assembles weekly, confers, and decides on a course of action to resolve information security and privacy breaches.

(3) Confirms status of information security and/or privacy breaches.

(4) Approves or denies requests for initial notifications and credit protection offers to individuals affected by breaches.

(5) Reports to the VA CIO.

(6) Nominations for membership are made by the Under and Assistant Secretaries to the VA CIO. The chair of the IRCT is the Deputy Assistant Secretary for Information Protection and Risk Management within OI&T or their designee.

(a) Regional IRTs coordinate risk-based responses to information security or privacy incidents at the regional level. Regional IRTs are chaired by the Regional/Network Director, who charters and oversees response actions necessary for any incidents involving SPI within his/her Region/Network.

(b) Local IRTs coordinate risk-based responses to information security or privacy incidents at the local level. Local IRTs are chaired by the Facility Director or their designee. who reviews privacy and security breaches, ensures accurate and timely reporting of incidents and follow-up information is provided to regional or national IRCTs as requested, and follows-up with approved remediation efforts.

(2) Preparation for Incidents. Incident prevention is a fundamental component of incident response programs. The incident response team’s expertise should be valuable in establishing recommendations for securing systems. This section provides basic guidance on preparing to handle incidents and on preventing incidents.

Tools and Resources

Incident Communications and Facilities
Contact information for team members and others within and outside the organization (primary and backup contacts), such as law enforcement and other incident response teams; information may include phone numbers, e-mail addresses, public encryption keys (in accordance with the encryption software described below), and instructions for verifying the contact's identity.
Call-Back and Duty Officer Roster and contact information which includes phone numbers, mail groups, after hour access, and escalation information
Incident reporting mechanisms, such as phone numbers, e-mail addresses, and online forms that can be used to report suspected incidents; at least one mechanism should permit people to report incidents anonymously.
Pagers or cell phones to be carried by team members for off-hours support, onsite communications.
Encryption software to be used for communications among team members, within the organization and with external parties; software must use a Federal Information Processing Standards (FIPS) 140-2 validated encryption algorithm.
War room for central communication and coordination; if a permanent war room is not necessary, the team should create a procedure for procuring a temporary war room when needed.
Secure storage facility for securing evidence and other sensitive materials.
Incident Analysis Hardware and Software
Computer forensic workstations and/or backup devices to create disk images, preserve log files, and save other relevant incident data.
Laptops, may serve as easily portable workstations for activities such as analyzing data, sniffing packets, and writing reports.
Spare workstations, servers, and networking equipment, may be used for many purposes, such as restoring backups and analyzing malicious code; if the team cannot justify the expense of additional equipment, perhaps equipment in an existing test lab could be used, or a virtual lab could be established using operating system (OS) emulation software.
Blank media, such as encrypted thumb drives, CD-R's, and DVD-R's.
Easily portable printer can be used to print copies of log files and other evidence from non-networked systems.

Packet sniffers and protocol analyzers may be used to capture and analyze network traffic that may contain evidence of an incident.
Computer forensic software to analyze disk images for evidence of an incident.
DVD-R's and CD-R's with trusted versions of programs to be used to gather evidence from systems.
Evidence gathering accessories, include hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions.
Incident Analysis Resources
Port lists, including commonly used ports and Trojan horse ports.
Documentation for Operating Systems, applications, protocols, and intrusion detection and antivirus signatures.
Network diagrams and lists of critical assets, such as Web, e-mail, and File Transfer Protocol (FTP) servers.
Baselines of expected network, system and application activity.

Roles: Preparing for Incidents

VA Department	1. Establish a Department Incident Response Capability (VA-NSOC) for reporting, defining, tracking, validating, and providing assistance to the field for all privacy and security incidents, and events. 2. Establish an Incident Resolution Core Teams at a local, regional, and national level that coordinates a risk-based response to privacy and security incidents. 3. Establish the VA Office of Risk Management and Incident Response (VA-RMIR) that implements and follows up on decisions of the IRCT. 4. Maintain the Office of Privacy and Records Management and the Office of Cyber Security to provide policy, procedures, and guidance to the Privacy Officers (PO) and Information Security Officers (ISO) in the field for handling incidents.
VA-NSOC	1. Maintain contact information for team members and others within and outside VA, such as law enforcement and other incident response teams. 2. Ensure the field has appropriate incident response mechanisms, such as phone numbers, e-mail addresses, and tools available to report suspected incidents. 3. Ensure that the VA-NSOC staff is adequately trained to handle incidents and to assist the field. 4. Implement all appropriate devices, software, and Standard Operating Procedures (SOPs) that will pro-actively provide the information to prevent an incident, or keep it from growing into a larger incident and alert appropriate personnel about the potential or actual incident in a timely manner. 5. Staff and train a Enterprise Security Management Team to provide the necessary evidence collection, forensics or containment actions as necessary.
Under Secretaries, Assistant Secretaries, and Key Officials	1. Ensure that all users of VA information and information systems under their responsibility take annual security and privacy training. 2. Ensure that employees support and comply with the incident response process. 3. Ensure appropriate Regional and Local IRTs are established within each organization.
IRCT	1. Provides advance planning, guidance, analysis and recommendations to the VA CIO, Regional Directors, local Directors and VA senior management to properly address and mitigate incidents involving the loss or compromise of data within VA custody. 2. Drafts quarterly and ad hoc reports to Congress. 3. Is responsible for data breach mitigation.
Chief Information Officers	1. Ensuring the establishment of Facility IRCT in accordance with Directive 6500. 2. Maintain as current facility IRCT contact information. 3. Make training available as is appropriate and necessary to facility IRCT. 4. Ensuring that all users of VA information and information systems

	under their responsibility take annual security and privacy training. 5. Working closely with the facility ISO to maintain continuity of service. 6. Ensuring that all users of VA information and information systems under their responsibility take ownership/responsibility for the data at their disposal. 7. Provide updates to open incidents as directed.
Privacy Officers	1. Take Privacy Officer Training 2. Take the Cyber Security Awareness course. 3. Obtain and maintain a Privacy Violation Tracking System (PVTS)/Remedy account and develop familiarity with the PVTS system. 4. Review VA Handbook 6502.1, PVTS. 5. Review Privacy Violation Tracking System Basic User's Handbook. 6. Review Formal Event Review and Evaluation Tool (FERET) User's Guide. 7. Become aware of the privacy laws, regulations, and policies that affect your organization. 8. Ensure that individuals within your organization recognize you as the PO. 9. Acquire template of Incident Notification/Credit Monitoring letter. 10. Become familiar with and establish a working relationship with ISO for your organization.
Information Security Officers	1. In conjunction with the Facility CIO, provide updates to high risk incidents every 2 hours, moderate risk level incidents every 6 hours and low level incident tickets every 72 hours. 2. Obtain and maintain a REMEDY user account and obtain training in REMEDY and FERET. 3. Enter all reported incidents into REMEDY within one hour of receiving or identifying an incident. 4. Complete a FERET risk evaluation form at the time of reporting the incident and update information on each incident accordingly. 5. Review Formal Event Review and Evaluation Tool (FERET) User's Guide. 6. Complete ISO training. 7. Become aware of the security laws, regulations, and policies that affect the organization. 8. Ensure that individuals within the organization know who their ISO is. 9. Become familiar with and establish a working relationship with the Privacy Officer for the organization.
Supervisors	1. Complete annual training and ensure staff has completed the required training. 2. Sign the Rules of Behavior and ensure that staff has signed.
Users	1. Complete required training. 2. Sign the Rules of Behavior.

(3) <u>Preventing Incidents</u>. Keeping the number of incidents reasonably low is very important to protect the business processes of VA and improve on public opinion of VA's ability to apply sound security and privacy practices and procedures to the data entrusted to them by our nation's veterans. If security controls are insufficient, high volumes of incidents may occur. Following VA privacy and security policies and implementing appropriate security controls on VA systems will help prevent VA incidents.

Roles: Preventing Incidents

VA Department	1. Ensure there is a VA user awareness and training program to educate users on appropriate privacy and security procedures.
VA-NSOC	1. Ensure that VA's network perimeter is configured to deny all unauthorized activity. 2. Ensure that there is a VA-wide malicious code prevention program. 3. Configure all hardware and software to ensure that reporting and alerts are pro-active and effective in bringing abnormal conditions to the attention of the right people in a timely manner. 4. All incidents are followed-up with after-action reports that generate actionable items for management which are managed as a project with assignments, dates, and status to help prevent a similar occurrence. 5. Ensure processes are clearly written, tested, and updated on a regular basis and as conditions change in strategies, organizations, people, or devices.
Under Secretaries, Assistant Secretaries, and Key Officials	1. Implement and comply with all VA policies, directives and handbooks on privacy, security, and records management in regards to the use, disclosure, storage, transmission, and protection of VA information in their organization.
IRCT	1. Ensures that policies and directives regarding data confidentiality and protecting data from the risk of exposure to identity theft are up-to-date.
Chief Information Officers	1. Adhere to VA configuration standards to ensure appropriate workstation and/or server setup by: a. Hardware/software patch installation and maintenance b. Anti-virus software and patch installation and maintenance c. Appropriate configuration setup and maintenance 2. Ensure the appropriate user awareness and training programs are available on privacy and security procedures. 3. Ensure that users are aware of the reporting procedures and the security policies in place to protect information systems, employees, and property. 4. Conduct regular review of user level permissions to network shares. 5. Maintain a strong working relationship with the facility ISO.
Privacy Officers	1. Implement privacy policies and procedures. 2. Implement a monitoring system for agency compliance. 3. Establish an internal privacy audit program. 4. Monitor and report that individuals in their organization complete the appropriate annual Privacy Awareness training program(s). 5. Ensure that privacy issues, and concerns are communicated to and coordinated with appropriate parties. 6. Become aware of the systems in their organization that collect and/or

	maintain SPI. 7. Participate in the filing and updating of Privacy Impact Assessments for systems within the purview of their organization. 8. Understand what constitutes a Privacy Act System of Records (SOR), and ensure that all SPI that is retrieved by the individual's name or other unique identifier is contained in an official SOR. 9. Promote activities to foster privacy awareness (e.g. Privacy Day, Information Protection Week, etc.)
Information Security Officers	1. Advise users on proper security protocols to prevent incidents. 2. Provide training to staff on their role in preventing, reporting, and handling low-level security incidents. 3. Ensure systems and subsystems affected by incidents are isolated and, if necessary, are restored and/or rebuilt. 4. Provide local organization policy and procedures for reporting and handling incidents. 5. Ensure all users complete the VA Cyber Security Awareness training annually. 6. Ensure Rules of Behavior are signed annually. 7. Ensure that users know their ISO, and know when and how to report security incidents.
Supervisors	1. Comply with all directives and policies. 2. Provide an inventory of the affected software, documents, etc., with an operational impact assessment of the potential data compromise and to assist with investigations. 3. Ensure all subordinates complete Privacy Awareness Training and VA Cyber Security Awareness Training annually.
Users	1. Complete mandatory security and privacy awareness training on an annual basis. 2. Be alert to their surroundings and report any suspected incidents to their respective ISO and PO. 3. Be vigilant in watching for unusual system behavior that may indicate security incident in progress. 4. Comply with all directives and policies on the appropriate use and security of VA information.

5. DETECTION, REPORTING AND ANALYSIS

a. When a suspicious privacy or security event or situation has been detected or suspected by VA staff, it must be escalated to the appropriate level of the Department for resolution. Events escalated will be reviewed and evaluated to determine their risk level and potential impact. If they are found to constitute a security or privacy incident, an appropriately measured response will be taken.

b. After detection, incident and reportable event reporting follows two pathways in parallel: technical and management/oversight.

(1). The technical pathway is designed to assist with the handling of incidents and provide fixes to mitigate the operational and/or technical impact of an incident.

(2). The management and oversight pathway is designed to notify departments at all levels of the ability of their systems to support operations and the operational impact of the incident. The management and oversight pathway is also a conduit for the IRCT to plan the incident handling process to mitigate any additional negative impact on operations or breaches.

c. It is vital to begin documenting all details of the event or incident at this point as this will provide invaluable information to personnel as they try to unravel the course of events. Recording details provides evidence for potential litigation.

(1) <u>Incident Categories</u>. VA-approved categories of incidents is located in Appendix B. Appendix C provides specific VA examples of these categories of incidents.

(2) <u>Signs of an Incident</u>. Incidents may be detected through many different means. Automated detection capabilities include network-based and host-based intrusion detection systems, antivirus software, and log analyzers. Incidents are also detected through manual means, such as problems reported by users or veterans. Signs of an incident fall into one of two categories: indications and precursors. A precursor is a sign that an incident may occur in the future. An indication is a sign that an incident may have occurred in the past or may be occurring now.

a. Although no single symptom of a security incident is by itself, conclusive, observing one or more of these symptoms should prompt one to investigate events more closely.

(1) An indication from an intrusion detection tool

(2) Suspicious entries in system or network accounting

(3) Accounting discrepancies (e.g., someone notices a gap in the accounting log in which no entries appear.)

(4) Unsuccessful logon attempts

(5) Unexplained, new user accounts

(6) Unexplained, new files or unfamiliar file names

(7) Unexplained modifications to file lengths or/or dates, especially in system executable file

(8) Unexplained attempts to write to system files or changes in system files

(9) Unexplained modification or deletion of data

(10) Denial of service or inability of one or more users to login to a system

(11) System crashes

(12) Poor system performance

(13) “Door knob rattling" (e.g., use of attack scanners, remote requests for information about systems and/or users, or social engineering attempts)

(14) Unusual time of usage

(15) An indicated last time of usage of a user account that does not correspond to the last time that the user logged on

Roles: ***Detecting Incidents***

VA-NSOC	1. Hires and trains engineers to ensure familiarity with incident management systems and procedures. 2. Configures devices and software to provide appropriate alerts to the right people in a timely manner. 3. Provides root cause analysis systems and procedures to detect incidents. 4. Implements procedures that ensure that signs of incidents are escalated appropriately. 5. Actively monitor Intrusion Prevention Devices for suspicious activity. 6. Notifies field of security vulnerabilities in VA systems, and provides appropriate corrective actions.
Chief Information Officers	1. Implement national tools in a timely fashion. 2. Provide consistent monitoring and automated alert implementation. 3. Maintain a strong working relationship with staff to encourage reporting of incidents/suspected incidents.
Privacy Officers	1. Receive complaints from veterans or anyone within their organization who believes a violation of privacy has occurred. 2. Enter all complaints received into PVTS or the system allotted for the reporting of privacy complaints or violations within 1 hour of discovery. 3. Follow guidance provided by the VA Privacy Service in order to record all privacy complaints or potential violations in PVTS or the system allotted for the reporting of privacy complaints or violations. 4. Monitor all privacy complaints that they have entered into the system allotted for the reporting of privacy complaints or violations. 5. Provide updates to the system allotted for the reporting of privacy complaints or violations, as appropriate.
Information Security Officers	1. Initiate protective or corrective measures when an incident or vulnerability is discovered 2. Ensuring incidents are properly reported and that responses are coordinated; incident updates provided as required. 3. Coordinating with the Privacy Officer to determine if a security incident is also a privacy incident. 4. Ensure users are aware of when and how to report incidents.
Users	1. Observe their physical surroundings and making sure that no SPI data are left in an unsecured area. 2. Report any anomaly that they notice with their applications and computers. 3. Report any suspicion of inappropriate privacy or security practices.

d. Incident Reporting

(1) When a user of VA information and/or its systems observes a suspicious event or receives a complaint potentially involving VA sensitive information, the event or occurrence must be reported immediately to the facility's ISO and/or PO, as well as to his/her supervisor. If these individuals are not available, a user can report an event directly to the VA-NSOC's hotline number, which is available 24 hours a day, seven days a week. The number is 1-866-407-1566. An email can also be sent to vasoc@va.gov .When reporting, the user should provide as much information as possible, including:

(a) *Who* was involved in the event (include your own contact information)

(b) *What* exactly occurred? What information and equipment were involved?

(c) *Where* the event took place. Was it in a VA protected environment?

(d) *When* the event was discovered and by whom (date, time, time zone, and contact information).

(e) *How* many individuals may be potentially negatively impacted by the event.

(2) Some important tips for the user to remember in initial handling of events are:

(a) If it is a system event, do not shut down the workstation or system or disconnect it from the network without contacting and receiving instruction to do so from your ISO or PO. Don't continue to work on a PC or stay in an area where a security incident has been detected.

(b) Do not attempt to investigate whether data was accessed without permission – this is the responsibility of the OI&T staff, otherwise you may destroy valuable evidence.

(c) Do not talk to the news media. Refer all news media inquiries to your organization's Office of Public Affairs.

(3) Events potentially involving a breach of VA sensitive information may be communicated to the ISO, PO, and supervisor by any media, whether by person, phone, electronic or hardcopy. If you are sending VA sensitive information via e-mail, it must be encrypted. If sending it through the mail, the user must use the double envelope method.

(4) The listing for all of the ISOs and POs are also listed on the VA Intranet. Links to these resources can be found on the OI&T Information Protection Portal .

(a) The supervisor will contact the ISO and PO to confirm that the incident notification has been received.

(b) The ISO and PO will report it to the VA-NSOC and a determination will be made whether the event is a security or privacy incident or both.

(c) Depending upon the determination made in (4b), the PO or ISO will report the incident to local management, including local law enforcement and the local Office Inspector General (OIG).

(d) The ISO and/or PO must contact the VA-NSOC. The ISO will enter the incident via the VA Remedy system and the PO will report it to the VA-NSOC via the PVTS.

(e) In addition to entering the incident into the reporting tools above, the ISO and/or the PO will complete the information requested in the electronic Formal Event Review and Evaluation Tool (FERET) for those incidents involving a possible data breach. Each FERET form is then automatically attached to the ticket created by the ISO or PO. FERET instructions are available on the OI&T Information Protection (IA) portal.

(f) ISOs must also report the event to their respective Network ISO.

e. Incident Analysis

(1) An automated tool and process to assist in risk analysis has been developed for use throughout the IRTS. The diagram below (Fig 5-A) is a high-level representation of this Data Breach Incident Resolution Process. It is supported by the automated assessment tool called Formal Event Review Evaluation Tool (FERET). Using the FERET electronic risk assessment tool, and other determining factors, a data breach incident will be categorized by the local IRT into one of three tiers, corresponding to the appropriate risk level and mitigation. The categorization of the data breach incident will assist the IRT to determine the proper level of response.

Figure_5A.htm (Select this link for a text description of Figure 5-A)

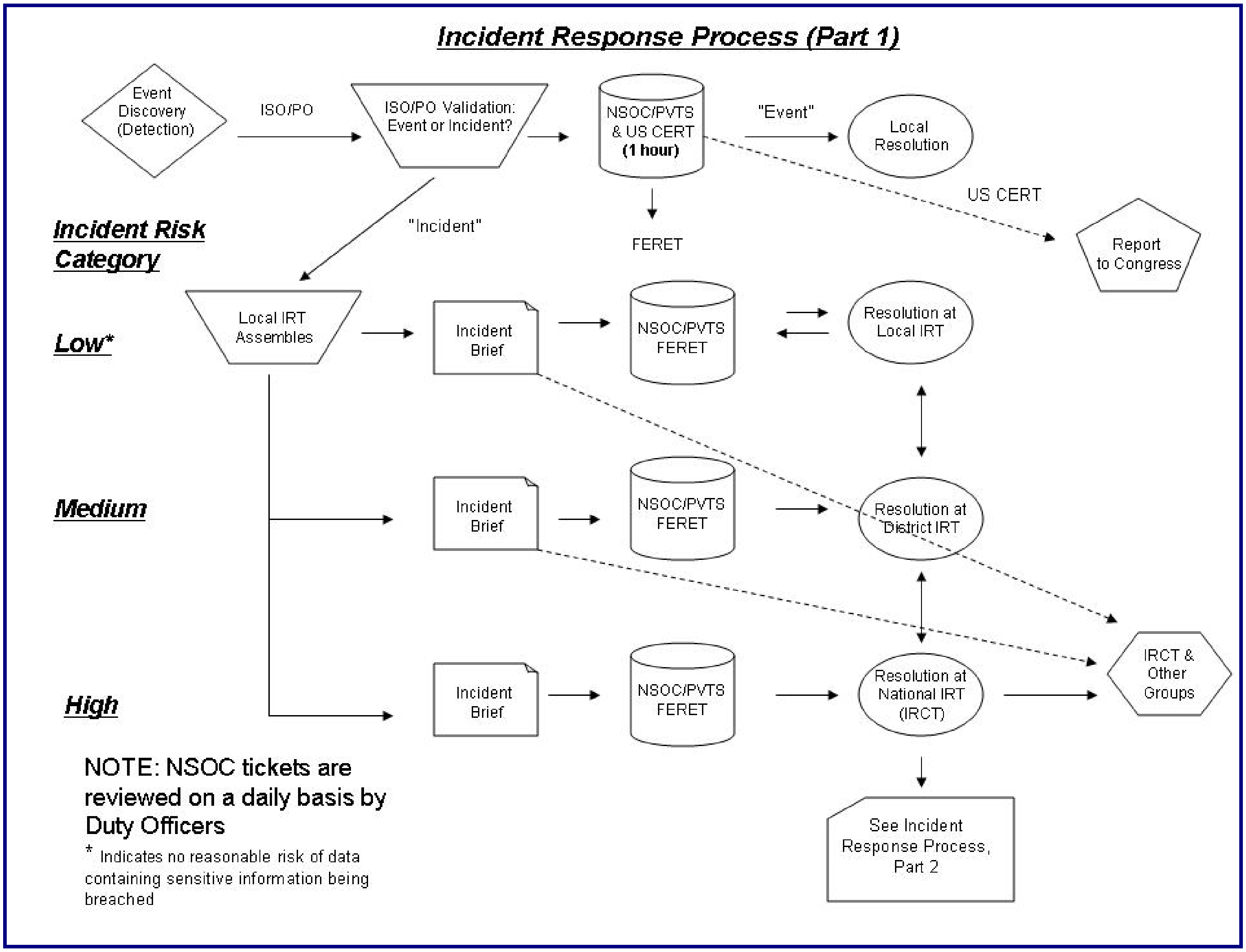

Incident Response Process (Part 1)
Event Discovery (Detection)
ISO/PO
ISO/PO Validation: Event or Incident?
NSOC/PVTS & US CERT (1 hour)
"Event"
Local Resolution
US CERT
Report to Congress
FERET
"Incident"
Incident Risk Category
Low*
Local IRT Assembles
Incident Brief
NSOC/PVTS FERET
Resolution at Local IRT
Medium
Incident Brief
NSOC/PVTS FERET
Resolution at District IRT
High
Incident Brief
NSOC/PVTS FERET
Resolution at National IRT (IRCT)
IRCT & Other Groups
See Incident Response Process, Part 2
NOTE: NSOC tickets are reviewed on a daily basis by Duty Officers
* Indicates no reasonable risk of data containing sensitive information being breached

Figure 5-A. Incident Response Process

(2) The FERET must be updated by the ISO or the PO as new information regarding the incident is obtained or at least every 3 days by the local IRT until the situation stabilizes.

(3) Upon determination that a reasonable risk of SPI misuse is evident it is necessary to notify veterans, their families, or employees of a possible breach of their personal information, the local IRT will use appendix G of this document. National credit monitoring contracts will be maintained and monitored by the IRCT. Each Under Secretary or Assistant Secretary's Office must promptly notify the VA-NSOC about the number and dates of credit monitoring notification letters mailed, and provide a copy of a redacted letter for the VA-NSOC archives to the VA IRCT mailbox.

(4) High risk FERET determinations, or significant data breach incidents may require that the local IRT or Regional IRT designate a person to be temporarily detailed to the IRCT to assist with remediation efforts.

(5) When a data breach incident occurs, the Incident Response Team at the facility that experience the incident engages in a preliminary analysis to obtain comprehensive and accurate information about the incident, determine the steps that must be taken, and then carries out the appropriate corrective action. The team at the national level the IRCT is generally involved as well. In the event of a major breach which will always involve the IRCT, the determination of corrective action will take place pending an independent risk analysis by a non-Department entity.

(6) As a result of the data loss in May 2006, new laws, policies, and other authorities were developed to establish clear and proper procedures deterring and responding to data breach incidents. The recent Department of Veterans Affairs Information Security Enhancement Act of which amended title 38 by adding Part 57, stipulates the following under 38 U.S.C. § 5724:

(a) If the Secretary determines, based on the findings of a risk analysis that a reasonable risk exists for the potential misuse of sensitive personal information involved in a data breach, the Secretary shall provide credit protection services in accordance with the regulations prescribed by the Secretary under this section.

(b) Regulations- Not later than 180 days after the date of the enactment of the Veterans Benefits, Health Care, and Information Technology Act of 2006, the Secretary shall prescribe interim regulations for the provision of the following:

1. Notification

2. Data mining

3. Fraud alerts

4. Data breach analysis

5. Credit monitoring

6. Identity theft insurance

7. Credit protection services

(c) Report- For each data breach with respect to sensitive personal information processed or maintained by the Secretary, the Secretary shall promptly submit to the Committees on Veterans' Affairs of the Senate and House of Representatives a report containing the findings of any independent risk analysis conducted, any determination of the Secretary, and a description of any services provided.

Roles: Incident Analysis

VA-NSOC	1. Provide a central coordination and incident management function for all incidents affecting the VA. 2. Validate that the occurrence of a security or privacy event is an incident. The VA-NSOC will attempt to validate all reported events in order to eliminate false positives. Validation will be via an investigative process and contacts. The VA-NSOC may request logs and other information in order to further validate the event. 3. If it is determined to be an incident involving a data breach, the VA-NSOC creates an Incident Tracking Ticket and notifies the IRT Falling Waters.
Incident Resolution Team (IRT-FW)	1. Identifying incidents involving data breaches by performing a daily triage on the Daily Incident Report provided by the VA-NSOC. 2. Coordinate and manage activities during incidents involving a data breach. This includes providing credit monitoring services promotion codes within 48 hours of a request from the Privacy Officer for the code. 3. Produce and maintain an incident communication plan coordinated with OPIA, OCLA, and OGC as necessary. 4. Provide the Administration and Staff Offices with a weekly report of incidents requiring notification and/or credit monitoring that is still pending action. This is prepared to assist the Administrations and Staff Offices to meet the 30 day turn around time after a data breach. 5. Facilitate and participate in incident reviews. 6. Ensures that a non-VA entity or VA's Office of Inspector General conducts an independent risk analysis to determine the level of risk associated with the data breach for potential misuse of any sensitive personal information involved in the data breach. 7. If it is determined that a reasonable risk exists for the potential misuse of sensitive personal information, VA shall provide credit protection services in accordance with regulations prescribed by the Public Law. 8. Contract for an independent risk analysis where warranted by the scale and severity of the incident. 9. Coordinate with other VA offices, as well as regional and local Incident Resolution Teams to assure the appropriate risk-based, tailored response for identity theft or privacy violation incidents within VA. 10. Work closely with other Federal agencies, offices, and teams. 11. Ensure Administrations and Staff Offices are aware of the Appeal Process fro requesting reconsideration from the IRCT when new information is obtained about an incident; and to request incidents be reopened if necessary.
Chief Information Officers	1. Maintain pertinent information including but not limited to audit and event logs as well as user account information when appropriate.

	2. Safeguard the integrity of involved hardware/software as appropriate.

f. <u>Incident Documentation</u>

(1) Every step taken from the time the incident was detected to its final resolution should be documented and time stamped. Emails containing SPI regarding an incident, as well as documents such as incident reports, should be encrypted so that only the sender and intended recipients can read them. The Microsoft Rights Management product and/or Public Key Infrastructure (PKI) will be used to ensure that access to incident information is properly restricted.

Roles: Incident Documentation

VA-NSOC	1. Track the progress of response activity via a security event trouble ticket, if the event is determined to be a security or privacy incident, and performing all necessary documentation of incident progress. 2. Update records about the status of incidents, along with other pertinent information.
Incident Resolution Team (IRT-FW)	1. Maintain records about the status of incidents, along with other pertinent information. 2. Maintain a detailed log of actions, as necessary, taken by all parties working the incident. This log is often referred to as a “Tic Toc” list. 3. Produce management information, as necessary, for significant events. 4. Produce incident progress updates, as necessary, for significant events.
Chief Information Officers	1. Remain in the information and communication chain. 2. Provide input as required in any documentation requested from top management both inside and outside the medical center. 3. Safeguarding data and sensitive information related to the incident. 4. Ensure that access to incident data is properly restricted.
Privacy Officers/ Information Security Officers	1. Enter updates to the system allotted for the reporting of privacy/security complaints or violations, as necessary, for any incident with a status of “Open”. 2. ISOs and POs will also receive an e-mail alert from the reporting tools reminding them to provide an update. If the ticket is in “pending” status, then an update is required after 1 week. 3. If the incident has a FERET risk category of “High” and has not been closed, then the ticket is included in the daily report of high-risk incidents that is sent to the Regional ISOs by the VA-NSOC. 4. These high risk tickets will be reviewed at least every 72 hours or until FERET scores are stabilized, and will be discussed during the weekly IRCT meeting. The ISOs and POs should immediately update the FERET form with new information about the incident as soon as it becomes available. FERET forms are available for update through the Remedy application at any time.

g. Incident Prioritization

(1) Basis of Prioritization. Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. They will be prioritized based on two factors:

(a) *Current and Potential Technical Effect of the Incident*. When handling an incident not only should the current technical impact be considered but also the future technical effect if the incident is not immediately contained. For example, a worm spreading among workstations may currently cause a minor impact, but within a few hours the worm traffic may cause a major network outage.

(b) *Criticality of the Affected Resources*. The criticality of the resource is based primarily on its data or services, users, trust relationships, and interdependencies with other resources, and visibility (e.g. a public web server versus an internal department web server).

(2) Process of Prioritization. Combining the criticality of the affected resources and the current potential technical effect of the incident determines the business impact of the incident.

(3) Levels of severity. The VA-NSOC uses a standardized, repeatable and reliable method to assess the severity of a security or privacy incident and report it to the United States Computer Emergency Readiness Team (US-CERT). The US-CERT is a partnership among the Department of Homeland Security and the pubic and private sectors established to protect the Nation's Internet infrastructure against and response to cyber attacks across the Nation. The initial step after gathering information is to assess its "severity" using the levels of low, medium, high and critical. The higher the severity level, the higher priority the VA-NSOC gives the issue. The four severity levels are:

(a) *Low* – any incident causing very low impact to VA's ability to perform its mission.

(b) *Medium* – any incident which poses a potential impact to VA's ability to perform its mission.

(c) *High* – any incident which poses an impact to VA's ability to perform its mission.

(d) *Critical* – any incident having a severe impact on the operational capacity of the Federal government.

(4) The VA-NSOC also uses the electronic FERET risk level determination along with other pertinent information regarding the incident will be used by the VA-NSOC to determine severity level. These severity levels help determine thresholds for prioritizing and escalating incidents. They will provide guidance for who will be notified and how aggressively notification and escalation shall be made. The nature of the information and its severity rating dictates the actions taken by the VA-NSOC. These severity assignments allow VA-NSOC to focus on issues that directly affect the overall confidentiality, integrity, and availability of VA information and its systems.

(5) Often, incidents require escalation. Escalation is a mechanism that assists the resolution of an incident within the agreed service targets. There are two forms of escalation: a) management, or hierarchical, escalation and b) functional escalation.

(1) Management, or hierarchical, escalation may be carried out at any stage during the incident life cycle if it is thought that the incident will not be resolved satisfactorily or in time. It is the responsibility of staff to escalate the incident to management as soon as an unsatisfactory or untimely resolution becomes likely. Escalation should be initiated sooner rather than later so that there is still time

for management to assess the situation and implement a corrective action. Corrective actions might be to allocate additional resources or to seek specialized skills from elsewhere, either within or external to the organization.

(2) The need for functional escalation is considered throughout the life of an incident. Functional escalation concerns transferring an incident to different support staff, who are better equipped to progress the incident and achieve a resolution within the agreed service targets. In a tiered support structure, this may involve transferring the incident from second- to third-line teams; while in a platform-based structure, this could be an allocation to more experienced staff within the team or allocation to a different team because the incident category is different from that first thought. Functional escalation also includes raising the incident with external support resources and vendors. All escalation actions are recorded on the incident record.

Roles: Incident Prioritization

VA-NSOC	1. The Director and the manager, VA-NSOC Incident management Team officially assign a severity level. This marks the official determination that a security and/or privacy incident has taken place. 2. If the event is determined not to be a security or privacy incident, it will be mitigated, the solution entered into the VA-NSOC's knowledgebase, quality assurance review accomplished, follow-up and lessons learned established, and the ticket closed.
IRCT	1. Oversight of medium, high, or critical incidents involving the loss or compromise of data. 2. The FERET is used to determine the prioritization and criticality of an incident; however the IRCT can escalate any incident regardless of the FERET or US-CERT rating.

h. <u>Incident Notification</u> During major incidents, the handling of communications can often become a major difficulty in its own right. The objective of the Communications Plan is to provide coordination of all communications during the life of the incident. The plan should cover:

(a) Who needs to be regularly updated

(b) Contact details for all parties requiring updates

(c) Different update messages may be required depending on the audience receiving the communication:

(1) Senior management update

(2) Update for all staff

(3) Update for users

(4) Update for partners

(5) Update for staff working on the major incident

(6) Press/media statement

(7) Update for emergency services/authorities

(d) How often each type of update is required and when the next one is due

(e) Who is authorized to release each different update statement.

(f) The mechanism by which each update will be communicated.

(g) The time of the next management team meeting.

Roles: Incident Notification

VA-NSOC	When required notify the: 1. Critical Infrastructure Protection Service (CIPS) Director. 2. Affected Network ISO. 3. Facility ISO and Technical POC. 4. Deputy CIO, NETWORK CIO. 5. Others as appropriate (US-CERT, Office for Computer Crimes, Law Enforcement). 6. VA OIG hotline if criminal activity is involved. 7. IRCT for incidents involving data breaches.
IRCT	1. When required notify the Secretary, Inspector General, and certain other VA officials, the Office of Management and Budget (OMB); the Committees on Veterans' Affairs of the Senate and House of Representatives; other Federal agencies that the Secretary considers appropriate; and the impacted individuals. 2. The Incident Resolution Core Team serves as liaison between the functional area(s) affected, VA organizations, and certain non-VA entities, including OMB, the Government Accountability Office (GAO), and Congress. 3. Fully integrate with already-established incident reporting and response processes and procedures of the VA Network and Security Operations Center (VA-NSOC), and will work closely with the VA-NSOC to provide timely and concise incident reports and synopses. These reports will be used to conduct a preliminary data breach analysis in order to make risk-based decisions regarding data breaches, potential identity theft, risk mitigation, and follow-up actions. 4. In the event of a major data breach, the IRCT will secure an independent risk analysis, then issue guidance regarding mitigation of associated risk, and concur with, or recommend, corrective actions to prevent a breach recurrence. 5. Teams within the Incident Response Team Structure (IRTS) will assist in analyzing, addressing and mitigating data breach incidents to ensure timeliness, uniformity, and visibility of VA responses. Additionally, VA must follow and report the results of all assessments, plans, and procedures required under Federal laws, regulations, executive instructions, and other legal authorities. 6. Teams within the IRTS are responsible for responding to data breach incidents and handling notification requirements from a collaborative perspective, whereby responsible parties will work together in formulating plans and guidance, as well as sharing best practices 7. Prepares the Quarterly Notice to Congress on Data Breaches. This reports the number of incidents involving exposure of SPI categorized by VHA Veterans Integrated Service Networks (VISN), VBA regions, and all others. It also identifies the incidents that do not meet the notification timeframe.
Information Security Officers / Privacy Officers	1. Notify and keep local management and support staff apprised of the incident.

6. CONTAINMENT, ERADICATION, AND RECOVERY

a. When an incident has been detected and analyzed, it is important to contain it before the spread of the incident overwhelms resources or the damage from the incident increases. Most incidents require containment, so it is important to consider methods of containment early in the course of handling each incident. Steps must also be taken to eradicate risk by removing the cause of the incident and restoring services to normal.

b. Containment involves limiting the scope and magnitude of an incident, rather than allowing the incident to continue in order to gain evidence for identifying and/or prosecuting the perpetrator. As soon as an incident is recognized, personnel should immediately begin working on containing the incident. Often, containment of the incident, event, or actions to mitigate the potential threat (e.g., taking the system offline, blocking the ports) is taken by the local OI&T staff early in coordination with the VA-NSOC to protect the system or network and to prevent any further contamination or intrusion.

c. In addition to the above, personnel work within their chain of command to determine whether sensitive information should be left on affected information systems or whether it should be copied to media and taken off-line. It may be best to move critical computing services to another system on another network where there is considerably less chance of interruption. A decision is made whether the system should be shut down entirely, disconnected from the network, or be allowed to continue to run in its normal operational status so that any activity on the system can be monitored.

(1) Choosing a Containment Strategy. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a wired or wireless network, disconnect its modem cable, and disable certain functions). Such decisions are much easier to make if strategies and procedures for containing the incident have been predetermined.

(a) Containment strategies vary based on the type of incident. For example, the overall strategy for containing an e-mail-borne virus infection is quite different from that of a network-based distributed denial of service attack. Criteria for determining the appropriate strategy include:

(1) Potential damage to and theft of resources

(2) Need for evidence preservation

(3) Service availability (e.g., network connectivity, services provided to external parties)

(4) Time and resources needed to implement the strategy

(5) Effectiveness of the strategy (e.g., partially contains the incident, fully contains the incident)

(6) Duration of the solution (e.g., emergency workaround vs. temporary workaround).

Roles: Containment Strategy

VA-NSOC	1. Coordinate, with IRCT, the response efforts. 2. Coordinate with network ISO and local ISOs and others as appropriate (US-CERT, law enforcement, Privacy Service, etc.). 3. Prepare situation updates on status throughout response efforts. 4. Conduct post mortem. 5. Recommend and coordinates containment actions. 6. Perform scans as necessary.
IRCT	1. Coordinate and advise in the execution of the containment strategy and efforts. 2. Make decisions about containment actions. 3. Coordinate response actions until the incident is resolved. 4. Report to senior VA officials on the status of the incident.
Chief Information Officers	1. Work with the OI&T staff to assure containment actions are performed in a timely & efficient manner.
Privacy Officers/ Information Security Officers	1. Participate in initiating containment actions. 2. Suggest alternate containment actions, as necessary.

(2) <u>Evidence Gathering and Handling.</u> Although the primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for legal proceedings. In such cases, it is important to clearly document how all evidence, including compromised systems, has been preserved.

Roles: Evidence Gathering and Handling

VA-NSOC	1. Assist law enforcement with the collection of evidence. 2. Document all evidence collected and preserved, including compromised systems. 3. Consult and coordinate with the OIG.
OI&T Oversight & Compliance	1. Perform additional investigation or actions as requested by the CIO or their designee.
IRCT	1. Ensure that proper procedures are followed. 2. Oversight of the chain of custody and overall process.
Chief Information Officers	1. Preserve of hardware/software as appropriate and requested. 2. Preserve of audit and event logs as appropriate.
Privacy Officers/ Information Security Officers	1. Direction will be provided by NSOC or law enforcement. 2. Begin fact-finding investigation once initial complaint is logged into PVTS/Remedy. 3. Consult with law enforcement as necessary. 4. Log all comments and details of their investigation into PVTS or the system designated for the reporting of privacy complaints and incidents.

(3) Identifying the Attacker. During incident handling, system owners and others typically want to identify the attacker. Although this information can be important, particularly if the organization wants to prosecute the attacker, incident handlers should stay focused on containment, eradication, and recovery. Identifying the attacker can be a time-consuming and futile process that can prevent a team from achieving its primary goal – minimizing the business impact.

(4) Eradication and Recovery. After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malicious code and disabling breached user accounts. For some incidents, eradication is either not necessary or is performed during recovery.

(a) The resolution and recovery process is responsible for ensuring that any identified workarounds or solutions are properly implemented in accordance with change and release management processes and that any additional recovery actions are then taken.

(b) Resolution actions are the actions taken to resolve the immediate cause of an incident. Using the change and release management process, incident management is responsible to monitor the progress of resolution actions and confirm that they were successful.

(c) Once resolution actions have been successfully implemented, then any recovery actions should be carried out. Recovery means restoring a system to its normal mission status. Recovery actions are taken once the resolution actions have been completed and all components are back in normal working order. Depending on the incident, the resolution and recovery actions may need to be carried out by different teams.

(d) The objective of the Restoration Plan is to provide a planned and coordinated approach to restore service. The plan is owned by the IRCT and should document the actions that need to be taken, who should carry them out, and when they should be completed. The plan is regularly updated throughout the life of the major incident, ensuring that old versions are kept as an audit trail.

(e) The Restoration Plan contains the following:

(1) Statement of the "problem" as known at this time

(2) Breakdown of the incident detailing components, interfaces, and likely causes of the issue

(3) High-level plan of how to verify or rule out each possible immediate cause

(4) Weighting of each possible cause based on likelihood and ease of confirmation, allowing the investigation of each possible cause to be given a priority

(5) Details of which investigative or resolving actions will be taken at this stage, based on the assigned priorities

(6) Details of who will carry out the investigative or resolving actions

(7) The timelines that each action should be carried out in, and the time of the next restoration team review meeting

Roles: Eradication and Recovery

VA-NSOC	1. Assist in system restoration. 2. Coordinate response actions with CIO. 3. Suggest a remediation strategy.
IRCT	1. For a major incident involving the loss of data, the IRCT holds an initial planning meeting with the restoration team, any staff members who have already been working on the incident, affected managers, and any other relevant technical specialists. If the staff is geographically diverse, this meeting may take the form of a teleconference or video conference. The objective of the meeting should be to agree both a restoration plan and a communications plan. 2. Reviews progress regularly. The purpose of the meetings is to keep all parties informed, discuss progress, and provide management escalation when required. Once a management review meeting has been held, progress update statements should be agreed and issued. 3. Facilitating the production and maintenance of the major incident restoration plan. 4. When an event appears to be long term in nature the Business Continuity Team will be engaged.
Chief Information Officers	1. Balance mission needs with recommended risk mitigation. 2. Coordinate with Network ISOs and staff to implement eradication and remediation actions. 3. Assure response actions are carried out by LAN/WAN managers. 4. Implement recommendations as appropriate. 5. Maintain a record of costs associated with repair, restoration, business disruption, and labor.

7. POST-INCIDENT ACTIVITY

a. Some incidents require considerable time and effort. Performing follow-up activity is one of the most critical activities in responding to incidents. Following up helps organizations improve their incident handling procedures as well as continue to support any efforts to prosecute those who have broken the law.

(1) <u>Questions.</u> One of the most important parts of incident response is also the most often omitted: learning and improving. Questions to be answered in the lessons learned process include:

(a) Exactly what happened, and at what times?

(b) How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?

(c) What information was needed sooner?

(d) Were any steps or actions taken that might have inhibited the recovery?

(e) What would the staff and management do differently the next time a similar incident occurs?

(f) What corrective actions can prevent similar incidents in the future?

(g) What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

b. The closure phase of the incident management process is responsible for confirming with the initiator that the incident had been resolved, ensuring that details of the incident and the resolution have been recorded, categorizing the closure and then closing the incident record.

(2) <u>Lessons Learned.</u> One of the most important parts of incident response is learning and improving. Holding post-incident meetings that cross team and organizational boundaries provides a mechanism for information sharing.

Roles: Lessons Learned

VA-NSOC	1. Document the incident, after-action report, lessons learned, and actionable items to prevent future occurrences, with assignments, completion dates, and status.
IRCT	1. Sponsor a “Lessons Learned” meeting, as needed, with all involved parties after an incident with the goal of improving security measures and the incident handling process itself. 2. Create a follow-up report for the incident that provides a formal chronological order of events. 3. Review and update incident response policies and procedures.
Chief Information Officers	1. Participate with the facility IRCT in a post mortem review of all documentation surrounding the incident/suspected incident. 2. Implementation of “best practices” as appropriate based on the review.
Privacy Officers/ Information Security Officers	1. Log resolution of incident. 2. Raise user awareness through lessons learned.

(3) <u>Using Collected Incident Information</u> Lessons learned activities should produce a set of objective and subjective data regarding each incident. Over time, the collected incident data will be used in several capacities. The data may provide VA information indicating systemic security weaknesses and threats, as well as changes in incident trends. The data can be used in the risk assessment process, ultimately leading to the selection and implementation of additional controls. Data will also provide information measuring the success of the incident response teams. Collecting data and developing metrics that measure the success of the IRCT in handling particular incidents and roll-up into an overview of incident-related measures.

Possible metrics include:

(1) *Number of Incidents handled.* This is best taken as a measure of the relative amount of work that the IRCT had to perform. It is more effective to produce separate incident counts for each incident category (e.g. lost equipment with SPI data).

(2) *Time per Incident.*

(a) Total amount of labor spent on the incident

(b) Elapsed time from the beginning of the incident to its resolution

(c) Elapsed time for each stage of the incident handling process (e.g. containment, recovery)

(d) How long it took the incident response team to respond to the initial report of the incident

(3) *Objective Assessment of Each Incident.* The response to an incident that has been resolved can be analyzed to determine how effective it was. Following are examples of performing an objective assessment of an incident:

(a) Reviewing reports and other documentation for adherence to established incident response policies and procedures

(b) Identifying which precursors and indications of the incident were recorded to determine how effectively the incident was handled

(c) Determining if the incident caused damage before it was reported

(d) Determining if the actual cause of an incident was identified

(e) Calculating the estimated monetary damage from the incident

(f) Identifying which measures, if any, could have prevented the incident

(4) *Subjective Assessment of Each Incident.* IRCT members should assess their own performance and the entire teams' performance. Annual and ad-hoc audits will be performed on incident response to identify problems and deficiencies that can be corrected. Audit evaluations will include, but not be limited to:

(a) Incident response policies and procedures

(b) Tools and resources

(c) Team model and structure

(d) Incident handler training and education

(e) Incident documentation and reports

(f) Review of the measures of success

(4) Evidence Retention. Evidence involving incidents should be maintained per the current standards and policies. The local facility is responsible for maintaining the evidence in a secure manner and ensuring that it is readily available on request.

8. INCIDENT MANAGEMENT ASSISTANCE

a. By following sound incident management guidelines and best practices we will continue to prevent and reduce the number of security incidents and data breaches. Remember, “Privacy is what we protect. Security is how we protect it.”

b. Keep up with the latest information at the OI&T Information Protection portal .This contains all of the Information Protection news, information and links to Certification and Accreditation, Policy, Privacy, VA-NSOC, Security Management and Reporting Tool (SMART), Field Security Services, Enterprise Security Solutions, and Training.

c. Questions on incident management guidelines and activities can be directed to the VA-NSOC, IRCT, or Regional and Local IRTs. For further information refer to the VA 6500, Information Security Program, directive and handbook.

Incident Handling Key Recommendations and Checklist

1. Some key recommendations for incident management are summarized below.

(a) Prevent incidents from occurring by ensuring that networks, systems, and applications are sufficiently secure. Preventing incidents is beneficial to the organization and also reduces the workload of the incident response team. Performing periodic risk assessments and reducing the identified risks to an acceptable level are effective in reducing the number of incidents. User, IT staff, and management awareness of security policies and procedures are also very important.

(b) Establish mechanisms for outside parties to report incidents. Outside parties may want to report incidents to the organization; for example, they may believe that one of the organization's users is attacking them. Organizations should publish a phone number and e-mail address that outside parties can use to report such incidents.

(c) Start recording all information as soon as the team suspects that an incident has occurred. Every step taken, from the time the incident was detected to its final resolution, should be documented and time stamped. Information of this nature can serve as evidence for potential litigation. Recording the steps performed can also lead to a more efficient and systematic, and less error-prone handling of the problem.

(d) Safeguard incident data. It often contains sensitive information regarding such things as vulnerabilities, security breaches, and users who may have performed inappropriate actions. The team should ensure that access to incident data is restricted properly, both logically and physically.

(e) Prioritize incidents by business impact, based on the criticality of the affected resources and the technical impact of the incident. Because of resource limitations, incidents should not be handled on a first-come, first-served basis. Instead, organizations should establish written guidelines that outline how quickly the team must respond to the incident and what actions should be performed, based on the incident's current and potential business impact. This guidance saves time for the incident handlers and provides a justification to management and system owners for their actions. Organizations should also establish an escalation process for those instances when the team does not respond to an incident within the designated time.

(f) Include provisions regarding incident reporting in the organization's incident response policy. Organizations should specify which incidents must be reported, when they must be reported, and to whom. The parties most commonly notified are the CIO, head of information security, local information security officer, other incident response teams within the organization, and system owners.

(g) Establish strategies and procedures for containing incidents. It is important to contain incidents quickly and effectively to limit their business impact. Organizations should define acceptable risks in containing incidents and develop strategies and procedures accordingly. Containment strategies should vary based on the type of incident.

(h) Follow established procedures for evidence gathering and handling. The team should clearly document how all evidence has been preserved. Evidence should be accounted for at all times. The team should meet with legal staff and law enforcement agencies to discuss evidence handling, and then develop procedures based on those discussions.

(i) Hold lessons learned meetings after major incidents. Lessons learned meetings are extremely helpful in improving security measures and the incident handling process itself.

2. The checklist below provides guidance for the initial handling of an incident.

Initial Incident Handling Checklist

DETECTION AND ANALYSIS	
1.	Determine whether an incident has occurred.
1.1	Analyze the precursors and indications.
1.2	Look for correlating information.
1.3	Perform research (e.g., search engines, knowledge base).
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence.
2.	Classify the incident using the categories presented in Section 2 (e.g., disruption of service, malicious code, and unauthorized access).
3.	Follow the appropriate incident category checklist; if the incident does not fit into any of the categories, follow the generic checklist.

Generic Incident Handling Checklist for Uncategorized Incidents

DETECTION AND ANALYSIS	
1.	Prioritize handling the incident based on the business impact.
1.1	Identify which resources have been affected and forecast which resources will be affected.
1.2	Estimate the current and potential technical effect of the incident.
1.3	Find the appropriate cell(s) in the prioritization matrix, based on the technical effect and affected resources.
2.	Report the incident to the appropriate internal personnel and external organizations.

CONTAINMENT, ERADICATION, AND RECOVERY	
3.	Acquire, preserve, secure, and document evidence.
4.	Contain the incident.
5.	Eradicate the incident.
5.1	Identify and mitigate all vulnerabilities that were exploited.
5.2	Remove malicious code, inappropriate materials, and other components.
6.	Recover from the incident.
6.1	Return affected systems to an operationally ready state.
6.2	Confirm that the affected systems are functioning normally.
6.3	If necessary, implement additional monitoring to look for future related activity.

POST-INCIDENT ACTIVITY	
7.	Create a follow-up report.
8.	Hold a lessons learned meeting.

EXAMPLES OF INCIDENTS THAT ARE REPORTABLE TO THE ISO/PO

	REPORTABLE INCIDENTS	**CLASSIFICATION IN NSOC**	**REPORTABLE TO VA POLICE?**
1.	A VA employee using another VA employee's individual password and/or account information (with the same user access privileges)	CAT 4: Improper Usage	NO
2.	A person outside of VA using a VA employee's individual password and/or account information	CAT 1: Unauthorized Access	Case dependent (if the password is passed on to others, the VA Police and OIG must be notified)
3.	Failure to protect passwords and/or access codes (i.e., taping codes to equipment to avoid memorizing)	CAT 4: Improper Usage	NO
4.	Leaving a workstation signed on/unattended; failure to log off	CAT 4: Improper Usage	NO
5.	Unauthorized use of external computer connections (i.e. modems)	CAT 1: Unauthorized Access	**YES**
6.	Installation of unauthorized software (screensavers, games, etc.)	CAT 4: Improper Usage	NO
7.	Indication of computer virus	CAT 3: Malicious code	NO
8.	Theft of computer equipment or software	CAT 1: Unauthorized Access	**YES**
9.	Inappropriate use of software, such as illegal copying of licensed computer software	CAT 3: Malicious code	**YES**
10.	Inappropriate use of the Internet	CAT 4: Improper Usage	Case dependent (i.e., child pornography should be reported to the VA Police and OIG)
11.	Inappropriate use of Electronic Mail	CAT 4: Improper Usage	NO
12.	Misuse or defacing government equipment	CAT 4: Improper Usage	**YES**
13.	Destruction or tampering with government equipment	CAT 1: Unauthorized Access	**YES**
14.	Asking unauthorized personnel to access your personal record/data	CAT 4: Improper Usage	NO
15.	Unauthorized personnel accessing a co-worker's data records in response to their	CAT 4:	NO

	request.	Improper Usage	

U.S. CRIMINAL CODE PERTAINING TO INFORMATION SECURITY

1. Criminal activity is any activity that violates Federal or State statutes, ordinances, or codes, and constitutes a criminal act under the law. The majority, but not all, of Federal criminal statutes are codified under title 18 United States Code (USC). State statutes and ordinances are varied, and some entries under the Code of Federal Regulations (CFR) state criminal penalties as well. In addition to the examples below, 18 U.S.C. 641 (theft) and 18 U.S.C. 1001 (false statement) are also frequently used in prosecuting crimes pertaining to information security.

2. Major statutes related to information security may be found on the Computer Crime and Intellectual Property Section website of the U.S. Department of Justice, for example:

(a) 18 U.S.C. § 1029. (Fraud and Related Activity in Connection with Access Devices)
(b) 18 U.S.C. § 1030. (Fraud and Related Activity in Connection with Computers)
(c) 18 U.S.C. § 1362. (Communication Lines, Stations, or Systems)
(d) 18 U.S.C. pt. I. ch. 119. (Wire and Electronic Communications Interception and Interception of Oral Communications)
(e) 18 U.S.C. pt. I, ch. 121. (Stored Wire and Electronic Communications and Transactional Records Access)
(f) 18 U.S.C. pt. II, ch. 206. (Pen Registers and Trap and Trace Devices)

3. Copyright and Related Offenses:
(a) 17 U.S.C. § 506(a) / 18 U.S.C. 2319 (Criminal Infringement of a Copyright)
(b) 18 U.S.C. § 2318 (Trafficking in Counterfeit Labels, Illicit Labels, or Counterfeit Documentation or Packaging)
(c) 18 U.S.C. § 2319A (Unauthorized Fixation of and Trafficking in Sound Recordings and Music Videos of Live Musical Performances)
(d) 18 U.S.C. § 2319B (Unauthorized Recording of Motion Pictures in a Motion Picture Exhibition Facility)
(e) Copyright Felony Act of 1992, Pub. L. No. 102-561, 106 Stat. 4233 (1992), Legislative History

4. Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (1998):
(a) 17 U.S.C. § 1201 (Circumvention of Copyright Protection Systems)
(b) 17 U.S.C. § 1202 (Integrity of Copyright Management Information)
(c) 17 U.S.C. § 1204 (Criminal Offenses and Penalties)

5. Trademark Offenses: 18 U.S.C. § 2320 (Trafficking in Counterfeit Goods or Services)

6. Economic Espionage Act of 1996 (18 U.S.C. § 1831 et seq.);
(1) 18 U.S.C. § 1831 (Economic Espionage)
(2) 18 U.S.C. § 1832 (Theft of Trade Secrets)

7. Other Offenses Often Applicable in Information Security Cases:
(1) 18 U.S.C. pt. I, ch. 63 (Mail Fraud)
(2) 18 U.S.C. § 1343 (Fraud by Wire, Radio, or Television)
(3) 18 U.S.C. pt. I, ch. 119 (Trafficking in Interception Devices)
(4) 47 U.S.C. § 553 (Unauthorized Reception of Cable Service)
(5) 47 U.S.C. § 605 (Unauthorized Publication or Use of Communications)

REFERENCES

1. Statutory References

a. E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, (codified at 44 U.S.C. §§ 3601-06.

b. Privacy Act of 1974, 5 U.S.C. § **552a (1974)**

c. Federal Information Security Management Act of 2002 (FISMA), Pub. L. No. 107-347, 116 Stat. 2946, codified at 44 U.S.C. §§ 3541-3549

d. Department of Veterans Affairs Information Security Enhancement Act of 2006, Pub. L. No. 109-461, 120 Stat. 3450, codified at 38 U.S.C. §§ 5721-28.

e. Information Security Matters, 38 C.F.R. §§ 75.111-119

f. GAO-06-866T, Leadership Needed to Address Weaknesses and Privacy Issues at Veterans Affairs, (June 14, 2006).

g. Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization and Protection (Dec. 17, 2003).

2. Office of Management and Budget (OMB)

a. OMB Circular A-130, Management of Information Resources, Appendix III, Security of Federal Automated Information Resources (Nov. 28, 2000).

b. OMB Memorandum (M-05-08), Designation of Senior Agency Officials for Privacy (Feb. 11, 2005).

c. OMB Memorandum (M-06-16), Protection of Sensitive Agency Information (June 23, 2006).

d. OMB Memorandum (M-06-19) Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments (July 12, 2006).

e. OMB Memorandum (M-06-15), Safeguarding Personally Identifiable Information (May 22, 2006).

f. OMB Memorandum (M-07-16), Safeguarding Against and Responding to the Breach of Personally Identifying Information (May 22, 2007).

g. OMB Memorandum (M-06-20), FY2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (July 17, 2006).

h. OMB Memorandum, Recommendations for Identity Theft Related Data Breach Notification (Sept. 20, 2006).

3. Associated VA Directives and Handbooks

a. VA Directive 6502, Privacy Program.

b. VA Directive and Handbook 6500, Information Security Program.

c. VA Handbook 6502.1, Privacy Violation Tracking System (PVTS).

d. VA Memorandum, Operational Control of Cyber Security and Privacy Incidents.

e. VA Office of Information & Technology (OI&T), Formal Event Review and Evaluation Tool (FERET) User's Guide.

f. VA Office of Inspector General (OIG) Report No. 06-02238-163, Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans (July 11, 2006).

g. VA Network and Security Operations Center (VA-NSOC), Use of the VA-NSOC Application Through the Web Interface (Mar. 2007).

h. VHA Handbook 1605.1, Privacy and Release of Information (May 17, 2006).

i. VHA Handbook 1605.2, Minimum Necessary Standard for Protected Health Information (Apr. 9, 2003).

j. VA Secretary's Memorandum, Cyber Security is everyone's responsibility (Mar. 16, 2004).

4. National Institute of Standards and Technology (NIST) Publications

a. NIST Special Publication 800-53, Information Security: Recommended Security Controls for Federal Information Systems, Rev 2 (Dec. 2007).

b. NIST Special Publication 800-61, Computer Security and/or Privacy Incident Handling Guide; Recommendations of the national Institute of Standards and Technology (Jan. 2004).

ACRONYMS

1. **CIPS –** Critical Infrastructure Protection Service

2. **FERET –** Formal Event Review and Evaluation Tool

3. **FISMA** - Federal Information Security Management Act of 2002

4. **HIPAA –** Health Insurance Portability and Accountability Act of 1996

5. **IRA** – Independent Risk Analysis

6. **IRCT** - Incident Resolution Core Team also referred to as the Incident Resolution Team at the National level.

7. **IRM –** Information Resource Management

8. **IRT** – (Local or Regional) Incident Response Team

9. **IRT-FW –** (National) – Incident Resolution Team – Falling Waters

10. **IRTS** - Incident Resolution Team Structure

11. **ITOC** – OI&T Oversight and Compliance

12. **FISO –** Facility Information Security Officer

13. **IA** – Information Assurance

14. **ISO** – Information Security Officer (local)

15. **ISO OPS –** Information Security Officer for Field Operations

16. **IT** – Information Technology

17. **NCA –** National Cemetery Administration

18. **NETWORK CIO** – VISN Chief Information Officer

19. **NISO** - (Network) Information Security Officer

20. **NSOC –** Network and Security Operations Center

21. **OIG –** Office of Inspector General

22. **OI&T** – Office of Information and Technology

23. **OMB** – Office of Management and Budget

24. **PHI** - Personal Health Information.

25. **PII** - Personally Identifiable Information. See Sensitive Personal Information.

26. **PKI** – Public Key Infrastructure

27. **PO** – Privacy Officer

28. **PVTS –** Privacy Violation Tracking System

29. **RISO –** Regional Information Security Officer

30. **RO –** (VBA) Regional Office

31. **SMI –** Summary of Major Incidents Report

32. **SOP –** Standard Operation Procedure

33. **SPI –** Sensitive Personal Information

34. **US-CERT** - United States Computer Emergency Readiness Team

35. **VA -** Department of Veterans Affairs. Authority: 38 U.S.C. § 501, 5724, 5727, 7906.

36. **VA CIO –** VA Chief Information Officer (the Assistant Secretary for Information and Technology)

37. **VA-OIG**- Veterans Affairs Office of Inspector General (also known as OIG)

38. **VA-NSOC** - Veterans Affairs Network and Security Operations Center

39. **VA-RM/IR –** VA Office of Risk Management and Incident Response

40. **VBA –** Veterans Benefits Administration

41. **VHA –** Veterans Health Administration

42. **VISN –** Veterans Integrated Service Network

DEFINITIONS

1. Covered Entity – an organization or individual that is covered by the compliance requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and is:

(a) A health care provider that conducts certain transactions in electronic form.
(b) A health care clearinghouse; or
(c) A health insurance plan.

2. Data (or Information) Breach - the loss, theft or other unauthorized access, other than those incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form that results in the potential compromise of the confidentiality or integrity of the data.

3. Data Breach Analysis - the process used to determine if a data breach has resulted in the misuse of sensitive personal information.

4. Denial of Service – an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. For example,

(a) An attacker sends specially crafted information packets to a Web server, causing it to crash.
(b) An attacker directs hundreds of compromised workstations external to the organization to send as many Internet Control Message Protocol (ICMP) requests as possible to the organization's network.

5. Event – any observable occurrence in a system or network. Examples of events are a user connecting to a file share, a firewall blocking a connection attempt, or a user sending electronic mail. Adverse events are events with a negative consequence, such as system crashes, unauthorized use of system privileges, defacement of a Web page, and execution of malicious code.

6. Identity Theft - a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation (per section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a)

7. Independent Risk Analysis - an analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach

8. Information Security Incident – a security incident involving either improper usage of or unauthorized access to SPI.

9. Improper Usage – occurs when a person violates acceptable computing use policies. For example, a VA staff member improperly disposes of computer storage media (such as a hard drive, CD-ROM or thumb drive) with VA SI stored on it, by simply throwing it in a dumpster.

10. Incident – an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The term incident means security incident as defined in 38 U.S.C. § 5727(18). (Also see Privacy Incident and Security Incident).

11. Information System – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual.

12. Malicious Code – a virus, worm, Trojan horse, Rootkit, Keylogger, or other type of computer code that is designed to compromise a host computer for malicious purposes.

13. Major Incident – An information security or privacy incident that involves serious and immediate risk of identity theft to more than 100 individuals.

14. Personally Identifying Information (PII) – any information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (see Sensitive Personal Information, below).

15. Privacy Incident - is a confirmed event in which information protected by HIPAA and/or the Privacy Act of 1974 has been exposed to individuals or entities that are not "covered entities" (see above), without the consent of the person to whom the information is pertaining.

16. Protected Health Information (PHI) – individually-identifiable health information, protected under HIPAA and the Privacy Act of 1974, including demographic information collected from an individual that is:

(a) Created or received by a health care provider, health plan, or health care clearinghouse;
(b) Related to the past, present, or future condition of an individual and provision of, or payment for health care; and
(c) Used to identify the individual or creates a reasonable basis to believe that it can be used to identify the individual.

NOTE: PHI does not have to be retrieved by name or other unique identifier to be covered by this Handbook (see Sensitive Personal Information, below).

17. Risk Assessment - an analysis to determine the scope, likelihood and severity of the results of a SPI breach, to determine its resolution at a local or district level.

18. Scans, Probes, and/or Other Attempted Access – attempts by users or information systems external to an information system security perimeter to breach that system via unauthorized means (typically telecommunication) in order to gain unauthorized access non-public information.

19. Security Incident - A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An incident, as it relates to this handbook, is defined as any event that has resulted in: unauthorized access to, or disclosure of, VA sensitive information; unauthorized modification or destruction of system data, reduced, interrupted, or terminated data processing capability; introduction of malicious programs or virus activity; or the degradation or loss of the systems confidentiality, integrity, or availability; or the loss, theft, damage, or destruction of an Veterans Administration (VA) asset or a VA IT resource.

20. Sensitive Personal Information (SPI) – with respect to an individual, SPI means any information about the individual maintained by an agency, including the following:

(a) Education, financial transactions, medical history (Protected Health Information – PHI), and criminal or employment history.
(b) Information that can be used to distinguish or trace the individual's identity (Personally Identifying Information – PII), including name, Social Security number, date and place of birth, mother's maiden name, or biometric records.

21. Unauthorized Access – when a person gains logical or physical access without permission to a network, system, application, data, or other resource.

22. VA Sensitive Data/Information - All Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.

DATA BREACH MITIGATION

1. Purpose

a. This establishes processes for managing data breach incidents within the US Department of Veterans Affairs (VA) for assessing risk, establishing a central management focal point, implementing appropriate policies and procedures, promoting awareness, and monitoring and evaluating policy and control effectiveness. The mission and responsibilities of the local, regional and national tiers of the Incident Resolution Team (IRT) are outlined below, as well as guidance for conducting incident response, incident resolution and incident closure/lessons learned for incidents that involve data breach.

b. The primary goal of managing data breaches is to provide prompt and accurate notification and remediation to those individuals whose Sensitive Personal Information (SPI) was lost or compromised in an incident, as well as to ensure continued public trust in VA as the guardian of the sensitive personal information with which we have been entrusted. Note that SPI includes both Personally Identifiable Information (PII) – the breach of which could lead to identity theft - and Protected Health Information (PHI), which is covered under the Health Insurance Portability and Accountability Act (HIPAA).

c. Prompt notification and remediation also involves close coordination, both within VA – through the activities of the Incident Resolution Team – and with entities outside of VA such as the Office of Management and Budget and Congressional committees (particularly in the event of a major incident). This provides guidelines to enhance coordination efforts for greater efficiency, accuracy, and promptness in communicating with individuals affected by VA information security and privacy incidents.

2. Background

a. OMB Memorandum Recommendations for Identity Theft Related Data Breach Notification, (Sept. 20, 2006), mandates that VA and other agencies implement response structures for the prompt response and resolution of incidents potentially leading to identity theft. As a result, the three-tiered IRT structure for the management of VA information security and privacy breaches has been established.

b. Compliance with the following laws, regulations and policy memoranda is provided through the processes outlined below (see section 7 for a more details on laws and regulations listed):

(1) OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, Attachment 3: External Breach Notification (May 22, 2007).

(2) Department of Veterans Affairs Information Security Enhancement Act of 2006, Pub. L. No. 109-461, 120 Stat. 3450, codified at 38 U.S.C. §§ 5721-28, and subsequent published regulations.

3. Scope

a. These processes apply to all VA offices and personnel, including Federal employees, contractors, consultants, students, and volunteers, who interface with, or in any way use, VA information systems. This is addressed particularly to the members of the Incident Resolution Team (at local, regional and national levels), who have the responsibility to respond to, resolve, and follow up on any breach of SPI that impacts VA.

b. This appendix will detail the following steps in the process of managing information security and privacy incidents:

(1) Incident response;
(2) Incident resolution; and
(3) Incident closure/lessons learned.

c. These three steps are the last steps of the overall VA incident management process, depicted in figure G-1.

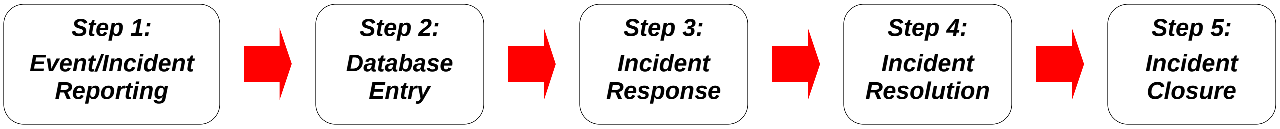


Figure G-1. VA Incident Management Procedure

Figure_G1.htm (Select this link for a text description of Figure G-1)

4. Roles and Responsibilities: VA Directive 6500, Incident Security Program, describes the responsibilities of VA senior officials, information owners, and information system users in VA incident management. In addition to these roles and responsibilities, this appendix adds the following:

ROLE	RESPONSIBILITY
VA Privacy and Information Security Officers (PO and ISO)	1. Report, monitor, and track incidents. 2. Enter and update information in PVTS or REMEDY, as well as in FERET. 3. Ensure timely closure of incidents.

Incident Resolution Team (IRT)	1. Coordinates a risk-based response to information security or privacy incidents at the local and regional level. 2. Assembles as necessary, confers, and decides on a course of action to resolve information security and privacy breaches. (See Figure 2-A for membership)
Incident Resolution Core Team (IRCT)	1. Coordinates a risk-based response to information security or privacy incidents at the national level. 2. Assembles weekly, or on an ad-hoc basis as needed, to confer, and decide on a course of action to resolve information security and privacy breaches. 3. Confirms status of information security and/or privacy breaches. 4. Determines need for initial notification and credit protection offers to individuals affected by breaches. 5. Coordinates media interfaces and contacts with other Federal agencies or outside entities. Reports to the VA CIO. (See Figure G-2 for membership)
VA Office of Risk Management and Incident Response (RM/IR)	1. Implements and follows up on decisions of the IRCT. 2. Performs analysis upon request. 3. Confers with other VA Senior Management officials and/or external authorities on major SPI breaches. 4. Manages contracts for all credit protection services, including data breach analysis and independent risk assessment. 5. Reports to the VA CIO.

Figure_G2.htm (Select this link for a text description of Figure G-2)

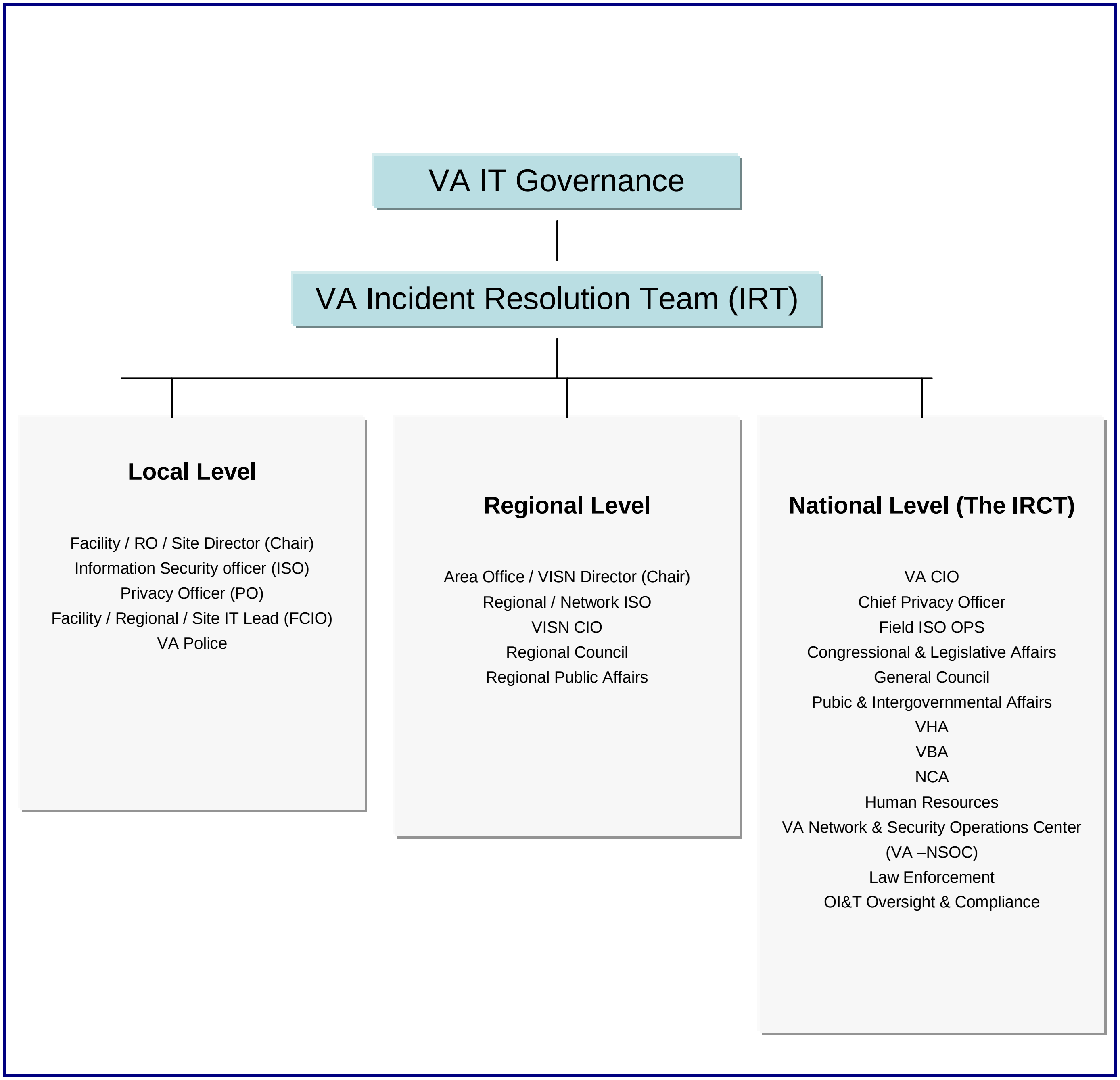

VA IT Governance
VA Incident Resolution Team (IRT)
Local Level
Facility / RO / Site Director (Chair)
Information Security officer (ISO)
Privacy Officer (PO)
Facility / Regional / Site IT Lead (FCIO)
VA Police
Regional Level
Area Office / VISN Director (Chair)
Regional / Network ISO
VISN CIO
Regional Council
Regional Public Affairs
National Level (The IRCT)
VA CIO
Chief Privacy Officer
Field ISO OPS
Congressional & Legislative Affairs
General Council
Pubic & Intergovernmental Affairs
VHA
VBA
NCA
Human Resources
VA Network & Security Operations Center
(VA –NSOC)
Law Enforcement
OI&T Oversight & Compliance

Figure G-2. VA Incident Resolution Team Structure

5. Management Process

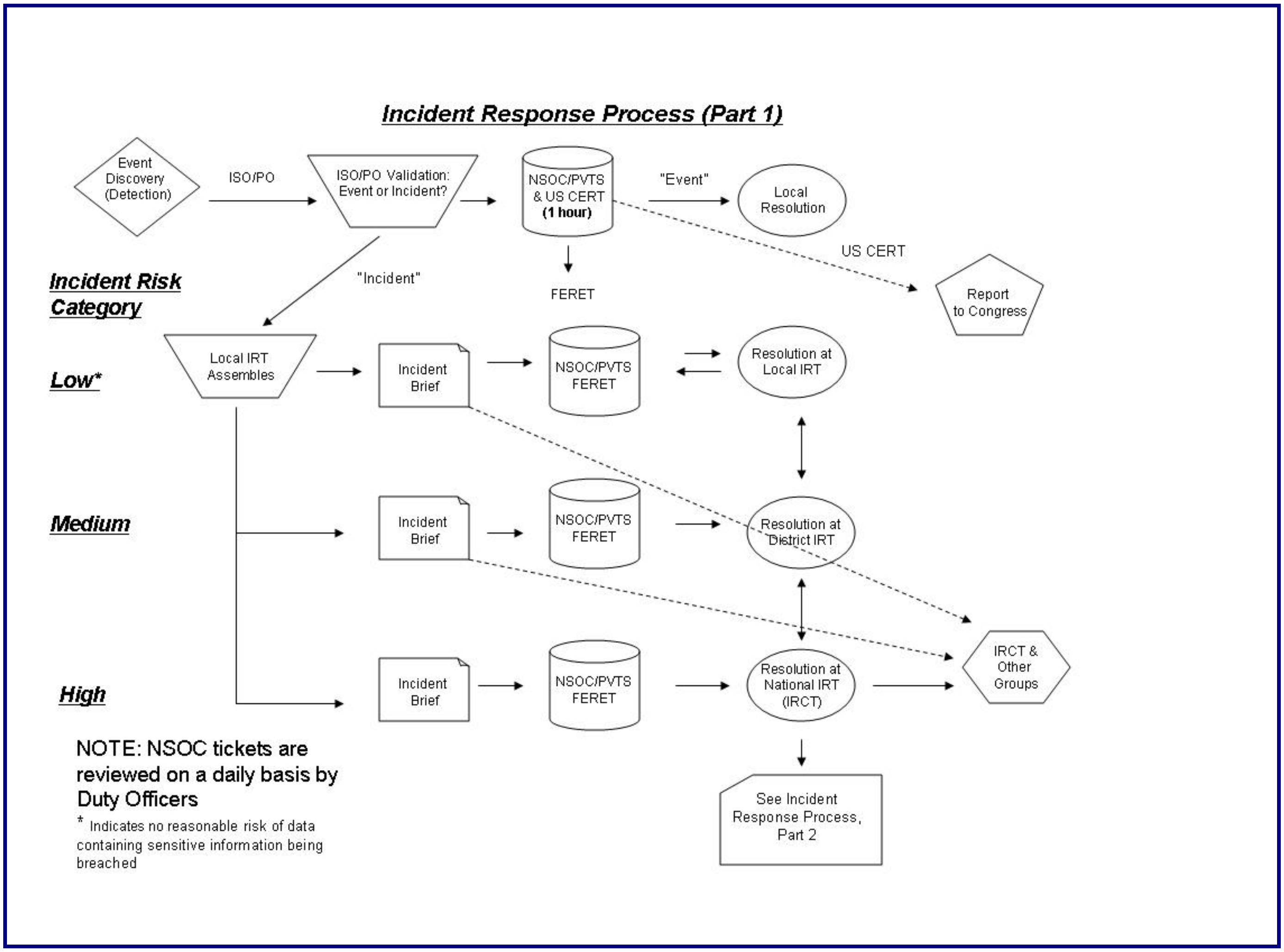
a. Incident Response

(1) The VA incident management process begins with local Information Security Officers (ISO) and Privacy Officers (POs) who verify potential information security and/or privacy events as incidents, and record them in either the NSOC, or PVTS, and FERET databases as appropriate. After these first two steps are completed, the Incident Resolution Team (IRT) at the local, regional and national levels has a wealth of information to draw upon in the process of incident management. Figure G-3 depicts the decision-making process that takes place within the IRT with regard to information security and privacy incidents.

(2) At the local and regional levels, IRTs may be convened any time there is a verified information security and/or privacy breach. The chair of the meeting oversees discussion of the breach – based upon the information entered in the NSOC/PVTS/FERET database –and charters direct action to mitigate the breach at the local or regional level, in coordination with all appropriate entities. Incidents that are confirmed at the local and regional level are followed by an Incident Brief, which is attached to the NSOC/PVTS/FERET ticket.

(3) The national tier of the IRT – known as the Incident Resolution Core Team (IRCT) – meets on a weekly basis and proceeds through the following tasks (illustrated in Figure G-4).

Figure_G3.htm (Select this link for a text description of Figure G-3)



NOTE: NSOC tickets are reviewed on a daily basis by Duty Officers

* Indicates no reasonable risk of data containing sensitive information being breached

Figure G-3. Incident Response Process (Part 1)

Figure_G4.htm (Select this link for a text description of Figure G-4)

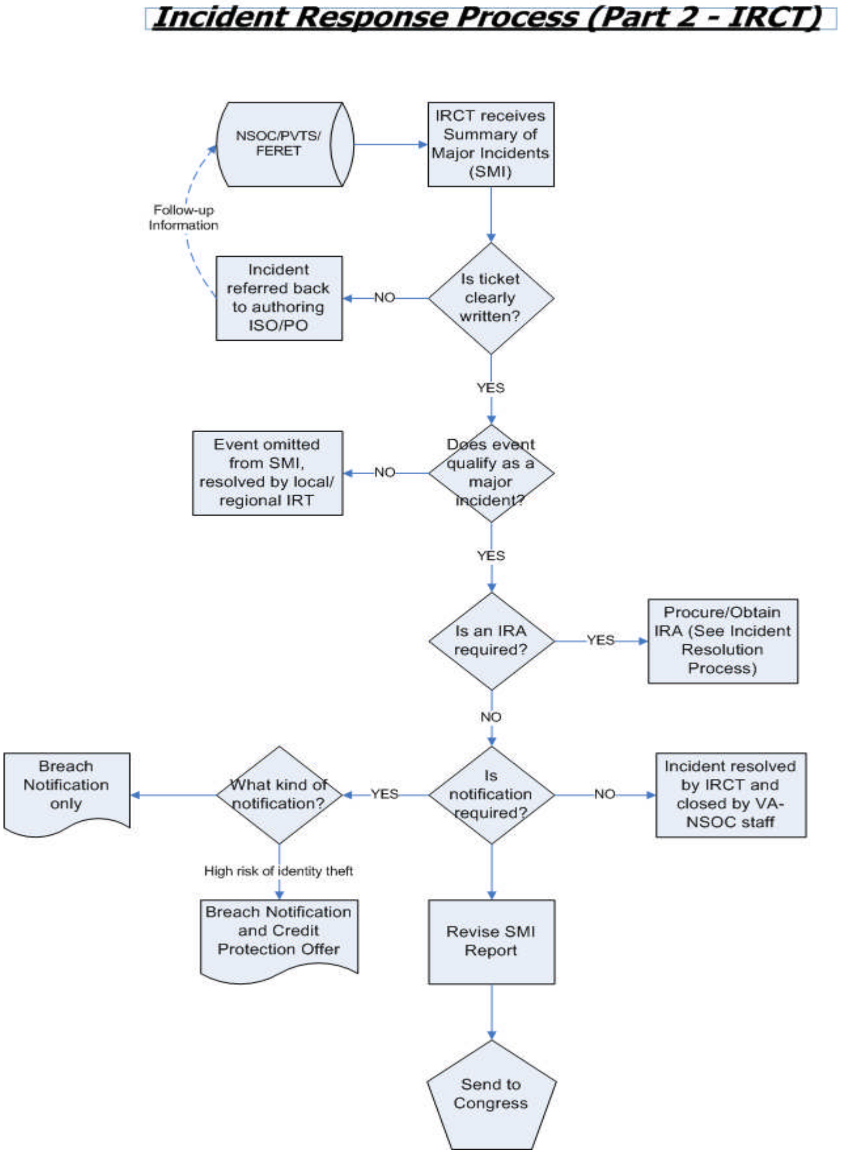

Incident Response Process (Part 2 - IRCT)
NSOC/PVTS/ FERET
IRCT receives Summary of Major Incidents (SMI)
Follow-up Information
Incident referred back to authoring ISO/PO
NO
Is ticket clearly written?
YES
Event omitted from SMI, resolved by local/ regional IRT
NO
Does event qualify as a major incident?
YES
Is an IRA required?
YES
Procure/Obtain IRA (See Incident Resolution Process)
NO
Breach Notification only
What kind of notification?
YES
Is notification required?
NO
Incident resolved by IRCT and closed by VA-NSOC staff
High risk of identity theft
Breach Notification and Credit Protection Offer
Revise SMI Report
Send to Congress

Figure G-4. Incident Response Process (Part 2)

(a) Database Triaging : The Falling Waters Incident Response Team daily review the entries in the NSOC/PVTS/FERET database that have been opened "scrubbing" them for clarity and internal consistency, and to determine whether or not further action is required to resolve the incident or mitigate potential harm. Those that warrant the IRCT's attention are included in the Summary of Major Incidents (SMI) report and reviewed at the weekly IRCT meeting. The IRCT may request follow-up information from any ISO or PO who has authored entries.

Note that cyber-security only events and incidents are also entered into the NSOC database; however, the IRCT does not normally deal with them in its meetings. The VA-NSOC staff responds to and resolves cyber-security incidents.

(b) Determine if Independent Risk Analysis (IRA) is Required: Each incident is reviewed to see if an IRA is required. According to the Veterans Benefits, Health Care and Information Technology Act of 2006 (Pub. L. No. 109-461, 120 Stat. 3450 (2006); 38 U.S.C. §§ 5724, 5727) an IRA may be waived and VA may proceed with offering credit protection service under three (3) circumstances (known as "Accelerated Response"):

1. If the IRCT (as empowered by the Secretary and VA CIO) judges that there is an "immediate, substantial risk of identity theft of the individuals whose data was the subject of the breach".

2. If a prior IRA conducted for VA on a breach of the same or similar data concluded that credit protection services should be offered; or

3. If a private entity with a similar breach would be required under Federal law to provide notification for the individuals affected.

a. If an IRA is required, then the VA Office of Risk Management and Incident Response (VA RM/IR) will obtain an IRA from a non-VA entity (whether from a contractor or another Federal agency) or from VA Office of Inspector General. If the IRA is waived, the IRCT proceeds to the next step.

(c) Determine if Notification is Required: The IRCT reviews the weekly significant data breach events and determines what actions should be taken to resolve each case. According to OMB Memorandum Safeguarding Against and Responding to the Breach of Personally Identifiable Information, Attachment 3: External Breach Notification (May 22, 2007) the following five factors should be taken into consideration when determining whether external notification is required for individuals affected by a VA information security and/or privacy incident:

1. Nature of the data elements breached;
2. Number of individuals affected;
3. Likelihood the information is accessible and usable;
4. Likelihood the breach may lead to harm:
a. Broad reach of potential harm;
b. Likelihood harm will occur;
c. Ability of VA to mitigate the risk of harm

(d) Determine What Type of Notification is Required: If notification is required, the IRCT then determines whether the notification should consist of:

1. A notification letter only of a privacy or security breach. This occurs if credit protection is not offered; if the need for credit protection is not yet known and timeliness dictates that notification be made, and when next-of-kin are notified of a data breach on a deceased individual.

2. Both a notification letter and an offer of credit protection service – According to OMB Memorandum Safeguarding Against and Responding to the Breach of Personally Identifiable Information, Attachment 3: External Breach Notification (May 22, 2007) the decision to offer credit protection services should be based on:

a. The data elements involved in the breach;

b. The number of individuals affected or potentially affected;

c. The likelihood that sensitive personal information will be or has been compromised (made accessible to and used by unauthorized persons);

d. The risk of harm to the affected individuals (the risk rating calculated by the FERET tool should help in this determination); and

e. The ability to prevent or mitigate the risk of harm by offering credit protection services.

(e) Revise Weekly Summary of Major Incidents (SMI) Report: On a weekly basis, the VA Office of Incident Resolution Team revises the SMI report for submission to Congress (see below, Communicating with Congress). The following types of information security and privacy incidents are examples of what should be retained on the SMI report that is submitted to Congress:

1. Incidents involving theft or missing hardware (regardless of whether or not SPI was stored on it);

2. Incidents involving communications (such as mail, faxes, and automated medical prescription deliveries) that include SPI and are mistakenly sent to a person(s) other than the intended recipient – these are “rolled up” in summary form.

b. Incident Resolution

(1) Incident resolution is the process of implementing action items in order to resolve information breaches, mitigate potential harm, institute corrective actions and to ensure the public’s continued trust in VA. Much of incident resolution involves proactive external communication – first to the people whose information was involved in the incident then to Congress and the general public. In addition to communication, prompt remediation actions, such as offering credit protection services for affected individuals, are also critical.

(a) External Communications:

1. Communicating with Individuals: Communication with individuals directly affected by an incident is a very important process – it is critical that the information that is sent to these individuals be both timely and accurate. This communication typically takes the form of either a notification letter or a letter offering credit protection services paid for by VA and prepared by the Privacy Officer or a Facility Director’s designee.

2. Communicating with Congress: Department of Veterans Affairs Information Security Enhancement Act of 2006 states that in the event of a breach involving SPI, VA must present a report containing the findings of any independent risk analysis (IRA) to the Committees on Veterans' Affairs of the Senate and House of Representatives. In the event of breaches involving active duty members, VA must also present the same report to the Armed Services Committees of the Senate and House. The IRA

will most likely be a service that is procured from a contractor external to VA, although an arrangement may be made with another Federal agency with expertise in this area.

a. Congress is also regularly apprised of VA's information security and privacy breach remediation activities through weekly submission of the US-CERT report and the revised Summary of Major Incidents (SMI) Report.

b. All direct communication with Congress should take place through the Office of Congressional and Legislative Affairs.

3. Communicating with the General Public: In the event of a major information security incident, a toll-free phone line is to be established. The message being sent out via letter (notification or credit protection offers) or other public communication means is to be consistent with that being communicated through the toll-free line and should include reference to the toll-free line.

.

a. Media communications with the general public concerning incidents should be coordinated through the associated VA Public Affairs Office. VA staff and contractors should not speak directly to members of the press about any information security or privacy incidents, but should refer all inquiries to VA Public Affairs.

(b) Procurement of Remediation (Credit Protection) Services:

1. Under the Department of Veterans Affairs Information Security Enhancement Act of 2006, Pub. L. No. 109-461, 120 Stat. 3450: 38 U.S.C. §§ 5724, 5727, if an independent risk analysis (IRA) reveals a substantial risk of identity theft as a result of a VA information security incident (or if the IRA is waived under "Accelerated Response"), VA must offer credit protection services to the individuals directly affected. These services may include any or all of the following:

a. One year of credit monitoring services consisting of automatic monitoring of three relevant credit bureau reports;

b. Data breach analysis;

c. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution; and/or

d. One year of identity theft insurance.

2. VA RM/IR is responsible for establishing and maintaining any and all credit protection services provided by VA. This is to include, but not be limited to, credit monitoring, identify theft insurance, toll-free assistance lines and fraud resolution services.

3. When the IRTC determines that a notification letter or an offer of credit protection services is needed, the local facilities' Privacy Officer, or Facility Director designee, will draft the needed letters based on provided templates. The letters must be on VA letterhead paper. After the letters have been mailed, redacted copies are forwarded to VA IRCT Mailbox (vairctmailbox@va.gov) along with information on the number of letters mailed, the date mailed, and a request to have the incident ticket closed. The incident is not considered closed until the letters are received by the Mailbox and entered into Remedy. A weekly report of incidents requiring notification letters/credit monitoring that are still pending action is sent to assist the Administrations and Staff offices in meeting the 30 day turn around time for notification to veterans.

4. There are five types of notification letters. One, or more, of the following will be mailed for a given incident. Letters must be mailed within 30 days from the date the incident occurred.

a. HIPAA Only Notification Letter Template : This letter is sent to a living individual as notification that personal health information may have or has been exposed by VA without the individual's authorization (see figure G-5). This letter is not to be used in conjunction with a letter offering credit protection services.

b. Next-of-Kin Notification Letter Template: This letter is the only letter to be used when the individual is deceased (see figure G-6). Notification is made to the next-of-kin. This letter is not to be used in conjunction with a letter offering credit protection services, since credit protection is never offered to families of deceased individuals, regardless of the circumstances.

c. General Notification Letter Template: This letter is sent to a living individual as notification that personal information may have or has been compromised by VA (see figure G-7). This letter may be used whenever a letter offering credit protection services is also necessary.

d. Credit Protection Services Letter Template: This letter is sent to a living individual to provide an offer of free credit protection services (see figures G-8 and G-9). This letter is always mailed after, or in conjunction with, an initial notification letter. A unique enrollment code must be included in each letter.

e. All Clear Notification Letter Template: This letter is sent to provide notification that personal information has NOT been compromised by VA (see figure G-10). It is typically sent following the General Notification letter to clarify that no credit protection is required.

Department of Veterans Affairs

<PO Box>
<City, State, Zip>

<Name>
<Address>
<City, State, Zip>

Dear <Name>

I am writing to you, as the < Title > of the VA < Facility >, to inform you that I was recently notified that your health information may have been compromised. < Describe the incident, what occurred, when, and what PHI was involved. >

< Describe what has been/is being done to mitigate the loss or disclosure of PHI. Include local contact and phone number, if appropriate >

Other personally identifiable information, such as your social security number or date of birth, was not involved, so you are not exposed to identify theft due to this incident.

We take our responsibility to safeguard your health information very seriously. You have privacy rights under Federal law and regulation that protects your health information. If you are concerned that your privacy rights have been violated, you may file a complaint to the Secretary of the U.S. Department of Health and Human Services or to Veterans Health Administration (VHA). To file a complaint with VHA you may contact your VA health care facility Privacy Officer, the VHA Privacy Officer, or VHA via *Contact the VA* at http://www.va.gov or dial 1-877-222-8387. Complaints do not have to be in writing, though it is recommended. You will not be penalized or retaliated against for filing a complaint, because it is your right under the law.

You may find out more about your privacy rights by reading our *Notice of Privacy Practices*. You may obtain a paper copy of this notice from your local VA health care facility or you may download one at http://www1.va.gov/health/index.asp by clicking on “Privacy Practices Notice” under “Information for Patients.”

We at VA take our obligation to honor and serve America’s veterans very seriously. We believe the potential exposure of your personal health information was very limited; however, we wanted you to be aware of the situation. We apologize for any inconvenience or concern that this situation may cause.

Sincerely,

[VA to insert name, title, signature]

Figure G-5. HIPAA Notification Letter Template

Department of Veterans Affairs
<VA Name>
<Street>
<City, State, Zip>

<Name of NOK>
<Address of NOK>
<City, State, Zip of NOK>

Dear <Name of NOK>:

I am writing to you as the Director for <Name of VA in City, State>. You were recently notified that <General circumstances of the incident>. <Type of information>information regarding your deceased family member <Relationship> including their <specific information lost/stolen/inappropriately disclosed or used (e.g., name, social security number, amount billed and amount paid for services, etc.)>was disclosed. We have <remediation steps completed so far (e.g., done a physical search at all three locations, contacted OIG and FBI, etc.)> and have <Status (e.g., “not found the missing diskette”)>. We have already implemented <Type of ongoing remediation activities engaged in to date (e.g., a more secure mechanism for communicating billing information, etc)>.

Although we have no information to indicate this personal information has been misused, we are notifying you that you should be vigilant and take what you consider to be appropriate steps to protect your <Relationship's> estate against identity theft. If you should receive phone calls, e-mails, or other communications asking for personal information about your <Relationship's>you should verify that the request is valid and appropriate before deciding whether to provide any information. If you decide to provide information in response to such a request, you should provide only the information that you consider appropriate. More information that may be helpful is available on the internet from the Federal Trade Commission at http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html

One precaution we recommend is that a member of your <Relationship's>estate send a copy of the death certificate to all three (3) of the credit reporting agencies listed below. This will help to protect the identity of your <Relationship>.

Equifax
Office of Consumer Affairs
P.O. Box 105139
Atlanta, GA 30348

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-916-8800

If you have questions concerning this letter, please call <Name, Title, Phone Number>, you can write <Name> at <VA Name>, <VA Street, City, State, Zip>.

We at VA take our obligation to honor and serve America's veterans very seriously. We apologize for any inconvenience or concern this situation may cause, and we believe it is important for you to be fully informed of any potential risk to you.

Sincerely,
[VA to insert name, title, signature]

Figure G-6. Next-of-Kin Notification Letter Template

Department of Veterans Affairs
<VA Name>
<VA Street>
<VA City, State, Zip>

<Name>
<Address>
<City, State, Zip>

Dear <Name>:

I am writing to you as the Director for <Name of VA Facility in City, State>. We were recently notified that <General circumstances of the incident>. Your<Type of information>information including your<specific information lost/stolen/mis-disclosed or used (e.g., name, social security number, amount billed and amount paid for services, etc.)>was inappropriately disclosed. We have <remediation steps completed so far (e.g., done a physical search at all three locations, contacted OIG and FBI, etc.)> and have <Status (e.g., "not found the missing diskette")>. We have already implemented <Type of ongoing remediation activities engaged in to date (e.g., a more secure mechanism for communicating billing information, etc)>.

While we have no information to indicate this personal information has been misused, we are notifying you so that you may be vigilant and take appropriate steps to protect yourself against identity theft. If you should receive phone calls, e-mails, or other communications asking for personal information, always take caution and know who is requesting the information and its purpose.

If VA determines that your information or you are at risk as a result of this incident, VA will contact you shortly to offer credit protection services at no cost to you. If you are at risk, you will be notified in a follow-up letter how to obtain these credit protection services. In the mean time, one precaution we recommend is to request a free credit report from one or more of the three national credit bureaus by calling 1-877-322-8228. Information about this and other protections, including placing a "fraud alert" on your credit account, is available by calling the Federal Trade Commission at its toll free number, 1-877-438-4338, or by visiting its website,http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html.

If you have questions concerning this letter, please call <Name, Title, Phone Number>, you can write <Name> at <VA Name>, <Street, City, State, Zip>.

We at VA take our obligation to honor and serve America's veterans very seriously. We apologize for any inconvenience or concern this situation may cause, and we believe it is important for you to be fully informed of any potential risk to you.

Sincerely,
<Director Name>
<Title>

Figure G-7. General Notification Letter Template

Department of Veterans Affairs

<PO Box>
<City, State, Zip>

<Name>
<Address>
<City, State, Zip>

Dear [NAME]:

I am writing to you as the Director for <Name of VA Facility in City, State>. We were recently notified that <General circumstances of the incident>. Your<Type of information>information including your<specific information lost/stolen/mis-disclosed or used (e.g., name, social security number, amount billed and amount paid for services, etc.)>was inappropriately disclosed. We have <remediation steps completed so far (e.g., done a physical search at all three locations, contacted OIG and FBI, etc.)> and have <Status (e.g., “not found the missing diskette”)>. We have already implemented <Type of ongoing remediation activities engaged in to date (e.g., a more secure mechanism for communicating billing information, etc)>.

To help protect your identity from the risk of identity theft as a result of this incident, we have contracted with ConsumerInfo.com, Inc., an Experian® company, to provide you with one year of credit monitoring, at no cost to you. Please read the rest of this letter carefully because it explains the benefits for you in the one year of credit monitoring and how to apply for the credit monitoring.

Under Experian’s credit monitoring, they will monitor and alert you of key changes in your three national credit reports that may indicate fraudulent activity.

Please read this letter carefully. You will be asked for the Activation Code shown below to activate this service, regardless of the enrollment method you choose. Your complimentary 12 month membership includes:

- Monitoring all three credit reports with Experian®, Equifax®, and TransUnion® – everyday
- Your Experian, Equifax and TransUnion credit reports at sign up – free
- Unlimited access to your Experian credit report and score
- Notification alerts of key changes indicating possible fraudulent activity
- Dedicated team of fraud resolution representatives for victims of identity theft
- $25,000 identity theft insurance with no deductible provided by Virginia Surety Company, Inc.*

*Due to New York state law restrictions, identity theft insurance coverage cannot be offered to residents of New York.

Your credit monitoring activation code is XXXXXXXXX.

A. To sign up online, please visit www.consumerinfo.com/VA and follow the instructions. If you sign up online, all credit reports and alerts will be delivered via email.

B. To sign up by telephone, dial 1-888-829-6561. If you sign up by telephone, all credit reports and alerts will be delivered by the US Post Office.

C. To sign up by mail, complete the enclosed form and return it to the address indicated. If you sign up by mail, all credit reports and alerts will be delivered by the US Post Office.

To take advantage of the credit monitoring membership at no cost, you must enroll within ninety (90) days from the date of this letter. Your enrollment will be activated by mail, internet or telephone contact as explained above. According to Federal law, we are not able to activate this membership for you.

There are several additional steps you can take to further protect your credit. You may wish to check the Federal Trade Commission webpage at www.ftc.gov/bcp/edu/microsites/idtheft/index.html. You may also request a free credit report annually from each of the three credit reporting agencies. These reports can be obtained by visiting www.annualcreditreport.com or by contacting each of the three agencies directly at the phone number and addresses listed in this letter.

The credit reporting agencies, their addresses and telephone numbers are as follows:

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-916-8800

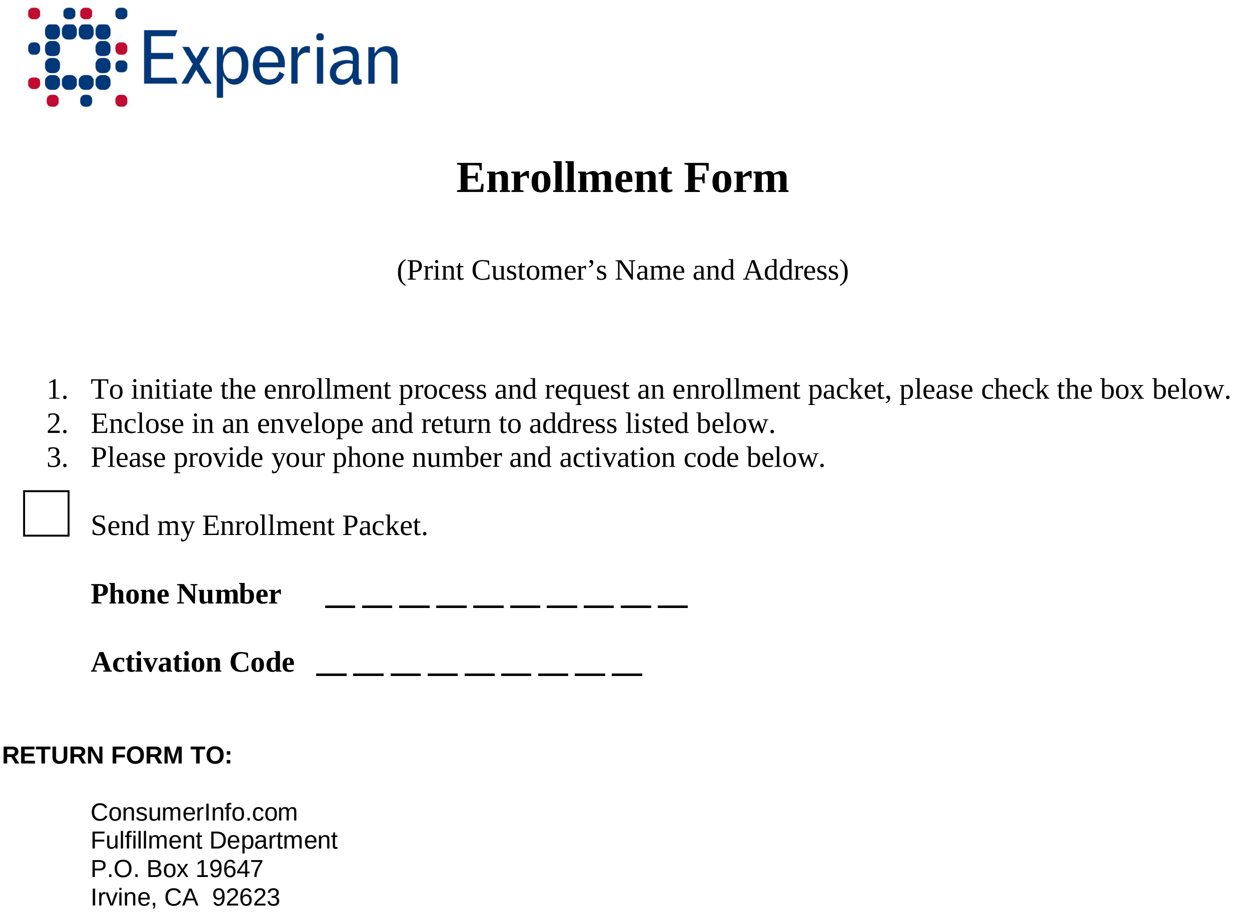
If you have any questions related to this incident contact (local VA facility phone number).

We sincerely apologize for any inconvenience or worry this may have caused you. VA is committed to protecting our veterans and we are constantly improving our processes to avoid any further reoccurrences.

Sincerely,
[VA to insert name, title, signature]

Figure G-8. Credit Protection Letter Template

Figure_G9.htm (Select this link for a text description of Figure G-9)



Experian

Enrollment Form

(Print Customer's Name and Address)

1. To initiate the enrollment process and request an enrollment packet, please check the box below.
2. Enclose in an envelope and return to address listed below.
3. Please provide your phone number and activation code below.

□ Send my Enrollment Packet.

Phone Number — — — — — — — — — —

Activation Code — — — — — — — — —

RETURN FORM TO:

ConsumerInfo.com
Fulfillment Department
P.O. Box 19647
Irvine, CA 92623

Figure G-9: Credit Protection Enrollment Form

Department of Veterans Affairs
<VA Name>
<VA Street>
<VA City, State, Zip>

<Name>
<Address>
<City, State, Zip>

Dear <Name>:

I am writing to you as the Director for <Name of VA Facility in City, State>. You recently received a letter notifying you that <General circumstances of the incident>. Since you received that notification, we have determined the extent of the incident and are pleased to inform you that your<Type of information>information was not disclosed. Our investigation of the incident determined that <general description of incident investigation and what data was exposed, if any.> We have already implemented <Type of ongoing remediation activities engaged in to date (e.g., a more secure mechanism for communicating billing information, etc)>

If you have questions concerning this letter, please call <Name, Title, Phone Number>, or you can write <Name> at <VA Name>, <Street, City, State, Zip>.

We apologize for any inconvenience or concern this situation may have caused you, but we acted on the assumption that you would rather be forewarned of the incident than to be kept uninformed until we had conducted a complete investigation. We at VA take our obligation to honor and serve America's veterans very seriously, including protecting the personal information with which we have been entrusted. In this case, we are pleased to let you know that your information is secure in our custody.

Sincerely,
<Director Name>
<Title>

Figure G-10: All Clear Notification Letter Template

5. The VA OI&T RM/IR maintains a national contract for credit protection services. When the IRCT determines that credit protection services will be offered, the individual is mailed a letter providing enrollment instructions, a mail-in enrollment form, and a unique enrollment code. The code is required by the credit protection company in order to provide the services at VA's expense.

6. Codes are requested by an ISO or PO sending an e-mail to *VA Identity Safety* (vaidentitysafety@va.gov). Enrollment codes will be distributed to the sender on an Excel spreadsheet. The following information needs to be included on the e-mail request for codes:

a. Number of codes needed (based on the total number of living individuals impacted by the incident).
b. Facility responsible for the incident.
c. The SOC ticket number of the incident.

7. Facilities should track all codes received and disbursed. It is important to record the date the codes are mailed, the ticket number involved, the name of the individual who is assigned a specific code, and the category of individual receiving the code (veteran, employee, DOD, etc.) If a letter is returned, it should be noted on the tracking spreadsheet after it is verified that VA did not make a mailing error. Every effort should be made to determine the correct address. If another address cannot be determined, the incident may closed. Your facility should maintain this spreadsheet on an ongoing basis in order to be able to identify the individual that received a specific code.

8. Appeals: Additional information about a given incident may become available after the IRCT has made a decision on the incident. In these cases, the person responsible for the incident ticket may appeal the decision by emailing the VA IRCT Mailbox (VAIRCTMailbox@va.gov). Appeals must be made within 10 days of the IRCT's initial decision and use the Appeals Request form (figure G-11). The IRCT will review the appeal and the VA-NSOC will notify the requester of the decision

APPEALS REQUEST FORM

Name of Appellant:

Phone number of Appellant:

Date of Request:

VANSOC Ticket Number:

PVTS Number:

Initial FERET score:

Current FERET score:

Initial Incident Summary:

What new information is available since the IRCT decision? (Be as detailed as possible):

Does the incident require notification? Yes No

Does the incident require Credit Protection? Yes No

Figure G-11: Appeals Request Form

c. Incident Closure and Lessons Learned

(1) The NSOC and the IRCT make the final determination that an incident is closed and the VA-NSOC staff note accordingly in the NSOC/PVTS/FERET database. As a general rule, an incident may be considered closed when either 1) the IRCT determines that no further action is needed, or 2) all affected individuals have been notified and/or offered remediation in response to the IRCT's decision on the incident and a copy of the redacted letter has been sent to the IRCT mailbox.

(2) Once an incident has been closed – particularly a major incident – the lessons learned from that incident are recorded, discussed, and best practices incorporated into the VA incident management process. There are several tools and forums to facilitate the incorporation of these lessons learned into standard practice, and to communicate these lessons to VA staff and contractors:

(a) **Incident Trend Analysis**: Using data from the NSOC/PVTS/FERET database, it is possible for the IRCT, VA RM/IR, and/or the Privacy Service – with the assistance of VA-NSOC – to extract and sort long-term data on VA information security and privacy incidents, illustrate trends using graphs or charts, and to make policy decisions based on these trends. For example, if a number of information security incidents are reported from a particular facility within a short time, it may indicate that either there is an IT system vulnerability at that facility or that there is a need for greater IT user education and awareness regarding information protection practices. The VA-NSOC regularly compiles weekly trend reports for submission to Congress along with the US-CERT.

(b) **Forums for Lessons Learned**: On at least an annual basis, cyber-security, information security and privacy staff (as well as outside guests) assemble to review major incidents and incident data from the past year and determine:

1. What trends can be observed over the past year?
2. What systemic weaknesses do these trends show?
3. Where was incident response and resolution the most effective? What actions were the least effective?
4. What best practices were discovered or displayed during these incidents?
Where can these best practices best be incorporated into the VA incident management process?

Lessons learned meetings are facilitated by the IRCT.

(c) **IT Training Venues**: Venues for the training of Federal IT security and privacy staff, as well as general IT users, are excellent opportunities to take lessons learned from past incidents and communicate them to stakeholders in the VA incident management process. Some examples of training venues include:

1. New VA employee orientation,
2. The INFOSEC information security conference, and
3. Training events sponsored by private sector organizations.

(d) **Policy Writing**: The chief way in which VA business practices are changed and improved is through written policy that is endorsed by VA senior management and distributed throughout the organization. So that lessons learned are effective, they are incorporated into VA IT policy directives, handbooks and standard operating procedures, and ultimately incorporated into VA staff training venues. Policy writing is a collaborative undertaking between divisions so that policy documents for cyber-security, information security and privacy are all consistent, accurate, and non-duplicative.

6. Compliance with Legal and Regulatory Mandates

(1) This process assures that the members of the Incident Resolution Team (IRT) (at all three tiers) can be quickly convened in the event of an information security or privacy breach that involves – or may involve – SPI. When such incidents occur, the IRT engages in a preliminary analysis to obtain comprehensive and accurate information about the incident, determines the steps that must be taken, and then carries out the appropriate corrective action.

(2) Once the IRT (or the national-level IRCT) has convened and confirmed that the incidents recorded in the NSOC/PVTS/FERET database are verifiable incidents, the IRT must make a decision as to a) whether or not to notify the individuals affected by the incident and b) what kind of notification should take place. Subsequent to its September 2006 memo, OMB issued Memorandum. Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007). Attachment 3 External Breach Notification," OMB requires that six elements should be addressed when considering notification of an information security incident to individuals external to VA:

(a) 5 factors should be considered to determine whether breach notification is required:
1. Nature of the data elements breached;
2. Number of individuals affected;
3. Likelihood the information is accessible and usable;
4. Likelihood the breach may lead to harm
a. broad reach of potential harm
b. likelihood harm will occur
5. Ability of the agency to mitigate the risk of harm

(a) Timelines of the notification;

(b) Source of the notification (typically the Agency Head or an individual designated by him/her);

(c) Contents of the notification – which should include:
1. A brief description of what happened, including the date(s) of the breach and of its discovery;
2. To the extent possible, a description of the types of personal information involved in the breach (*e.g.*, full name, Social Security number, date of birth, home address, account number, disability code, etc.);
3. A statement whether the information was encrypted or protected by other means, when determined such information would be beneficial and would not compromise the security of the system;
4. What steps individuals should take to protect themselves from potential harm, in any;
5. What the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and
6. Who affected individuals should contact at the agency for more information, including a toll-free telephone number, e-mail address, and postal address.

(e) Means of providing the notification; and

(f) Who receives notification (public outreach in response to a breach).

(3) In addition to the above six considerations, the recent Department of Veterans Information Security Enhancement Act of 2006 mandates that – prior to notification or offers of credit protection – the VA Secretary shall obtain an Independent Risk Analysis (IRA) by a "non-VA entity" to determine the probability that the breached SPI may be used to harm people affected by the breach.

(4) However, the subsequent final rule has also given the VA Secretary leeway to waive the IRA (as an "Accelerated Response") and proceed to offer credit protection services to individuals whose SPI has been exposed under three circumstances:

(a) If the Secretary judges that there is an "immediate, substantial risk of identity theft of the individuals whose data was the subject of the breach".

(b) If a prior IRA conducted for VA on a breach of the same or similar data concluded that credit protection services should be offered; or

(c) If a private entity with a similar breach would be required under Federal law to provide notification for the individuals affected.

(5) The law and the interim final rule also stipulate that – subsequent to findings of substantial risk by the IRA (or the IRA's waiver under "Accelerated Response") – the Secretary shall offer to provide credit protection services:

(a) These services may include any or all of the following:

1. One year of credit monitoring services consisting of automatic monitoring of three relevant credit bureau reports;
2. Data breach analysis;
3. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
4. One year of identity theft insurance.

(b) For each data breach, the Secretary shall submit the IRA findings and subsequent services provided to the Committees on Veteran's Affairs of the Senate and House of Representatives;

(c) For each data breach affecting active US military service members, the Secretary shall submit the IRA findings and subsequent services provided to the Armed Services Committees of the Senate and House of Representatives.

(6) Once a decision has been reach to offer credit protection, the interim final rule states that the type of credit protection services offered should be determined by the following considerations:

(a) The data elements involved in the breach;

(b) The number of individuals affected or potentially affected;

(c) The likelihood that sensitive personal information will be or has been compromised (made accessible to and usable by unauthorized persons);

(d) The risk of harm to the affected individuals; and

(e) The ability to prevent or mitigate the risk of harm by offering credit protection services.

(7) Finally, Department of Veterans Affairs Information Security Enhancement Act of 2006 states that in the event of a breach involving SPI, VA must present a report containing the findings of any independent risk analysis to the Committees on Veterans' Affairs of the Senate and House of Representatives. In the event of breaches involving active duty members, VA must also present the same report to the Armed Services Committees of the Senate and House.