# Security Information For NEDSS Base System States

## A Checklist For Security Protection

Prepared by the CDC NEDSS Project Team

Version 1.0
Effective Date January 16, 2002

# Table of Contents

# Security Information for NEDSS Base System Sites

## 1.0 Introduction

### 1.0.1 Purpose

The National Electronic Disease Surveillance System (NEDSS) project is a public health initiative to provide a standards-based, integrated approach to disease surveillance and to connect public health surveillance to the burgeoning clinical information systems infrastructure. NEDSS will improve the nation's ability to identify and track emerging infectious diseases (including potential bioterrorism attacks), investigate outbreaks, and monitor disease trends. Some states may choose to adapt existing systems to conform to the NEDSS architecture, others may choose to implement the NEDSS Base System (NBS) being developed by the CDC.

This document contains a series of questions designed to assist the NBS deployment team in understanding the state health department's security environment. While states choosing the NBS may wish to review the list and, perhaps, complete it before arrival of the team, it is designed to support a face-to-face discussion so that variations from standard security practices can be understood and evaluated. States implementing the NEDSS Architecture may also use this document as a guideline for a high-level security review of their implementation.

### 1.0.2 Security Overview

Because the NBS contains personal patient information, network security is extremely important. NBS sites must preserve patient confidentiality; meet state regulations regarding information privacy; provide secure exchange of information (messaging) across Internet connections; use industry-standard methods for authentication, access control, and encryption; support deployment within the security perimeter of adopting organizations without disturbing the existing network security systems (such as firewalls); and be compliant with HIPPAA standards.

Possible implementation options for the NBS include:

- Intranet only NBS: NBS installed on a local LAN that is not continuously connected to the Internet
- Intranet NBS in an Internet environment: NBS installed on a local LAN that is connected to the Internet, though the NBS itself is not accessible via the Internet
- Internet NBS: NBS accessible via the Internet using state-based strong authentication

Elements of the NBS sensitive to user security authentication and database protection include:

- NBS applications server
- Locally connected database supporting the NBS applications server
- Browser-based page "requested encrypted connection" to the NBS applications server from the agency's main Web server for a Secure Socket Layer (SSL) connection
- Local user intranet database access
- Direct Internet database access

To ensure database security integrity in either the intranet NBS in an Internet environment, or the Internet access environment, we recommend creating a de-militarized zone (DMZ) with firewall protection for both the State agency database and the NBS application server. Exhibit 1 shows a typical network enviroment and perimeter security configurations and the elements involved with systems and host server. The checklists indicated can be found in Section 2 of this document and are the minimum baseline security recommendations and specific risk vernability assessment questions needed to conduct an effective predeployment analysis for the NBS.

The red line shown in Exhibit 1 demonstrates a user accessing the Web server and shows SSL enablement, validation of the user, and SSL certificate validation taking place at the NBS applications server DMZ or domain. It is possible for a user to validate from his/her browser to the main site Web server only, however, that is where the encryption connection would stop. SSL or some other strong authentication is recommended for Internet NBS. It is more secure to extend the users request for the NBS application access via the Web server NBS user-access script. This would extend the process to the NBS application server where validation could then occur depending on the SSL vendor used. This allows for a full end-to-end encryption transaction.

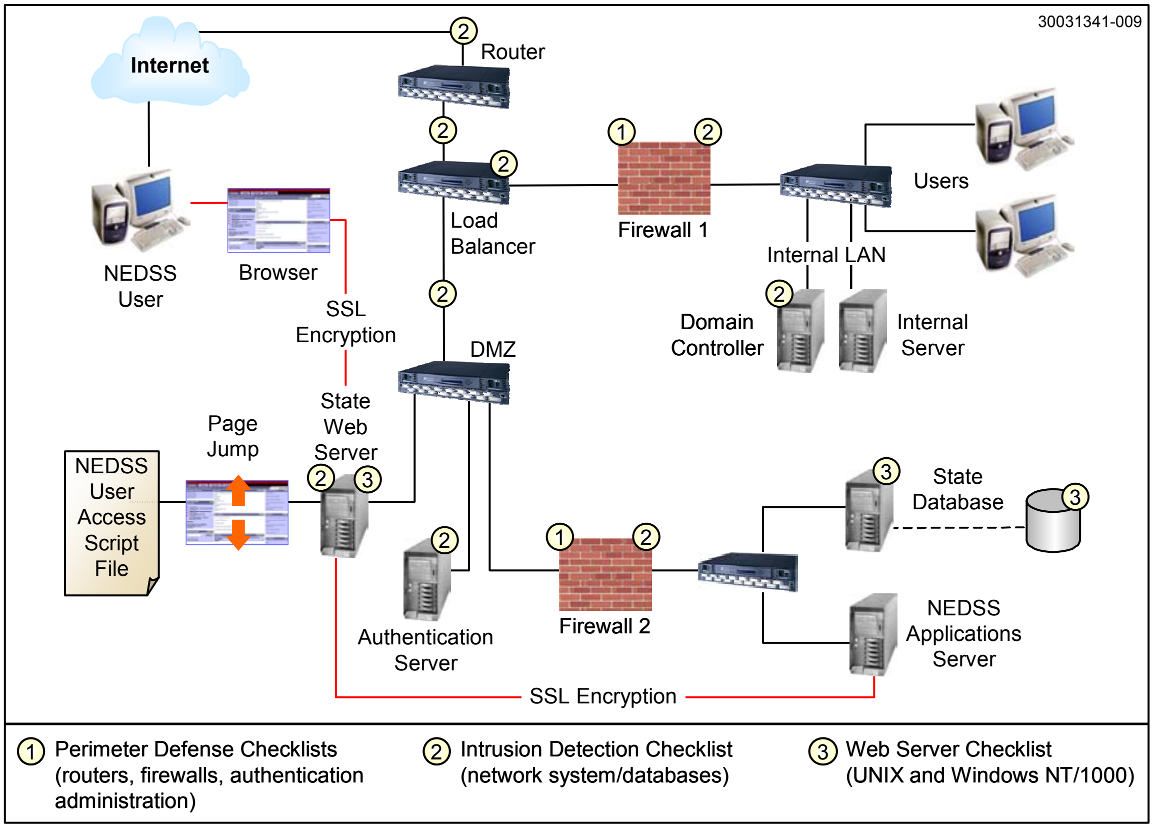
30031341-009
Internet
Router
Load Balancer
Firewall 1
Users
Internal LAN
Domain Controller
Internal Server
NEDSS User
Browser
SSL Encryption
DMZ
State Web Server
Page Jump
NEDSS User Access Script File
Authentication Server
Firewall 2
State Database
NEDSS Applications Server
SSL Encryption
1
2
3
① Perimeter Defense Checklists (routers, firewalls, authentication administration)
② Intrusion Detection Checklist (network system/databases)
③ Web Server Checklist (UNIX and Windows NT/1000)

*Exhibit 1. Typical Network Environment and Perimeter Security Configurations*

## 2.0 System Security Checklists

The following checklists provide security provision recommendations to ensure infrastructure and server integrity before deploying the NBS elements within the CDC and State environments. These are important steps that must take place early in the transition. **Items of special concern that have the potential to make the secure operation of the NBS difficult are shown in bold print in the checklist.**

□ 1. Which implementation does the state plan:

□ a. Intranet only NBS?

□ b. Intranet NBS in an Internet environment?

□ c. Internet NBS?

## 2.1 Perimeter Defense Checklists

Perimeter defenses include routers, firewalls, and authentication administration. Authentication is important regardless of the implementation selected, although strong authentication such as digital certificates are not so important in either of the intranet implementations. Firewalls are recommended for both the intranet NBS in an Internet environment, and the Internet NBS. Router filtering and logging can be helpful even in an intranet only NBS implementation to limit access from network nodes on the LAN that are not under strong physical security.

### 2.1.1 Routers

□ 1. **Extensive logging and frequent auditing of logs is generally considered a requirement for strong web security? Is logging enabled on your router? If so, what kind?**

□ a. **Does your router log packets that violate your filtering criteria?**

□ b. **Does your router support logging that adds information about the interface from which the packet was sent?**

□ c. How often are logs checked for "IP-directed broadcasts" that can be used in the extremely popular "smurf" denial-of-service attacks and other attacks designed to flood the network?

□ 2. Does the router system use access lists to filter traffic? If not, what mechanisms have been implemented to filter and/or monitor access?

□ a. **Is access verified by ensuring that the system received the MAC address of the host that sent it?**

□ b. **On a two-interface router connecting a corporate network to the Internet, are any datagram that arrives on the Internet interface but whose source address field claims that it came from a machine on the corporate network discarded? (This procedure prevents “spoofing”—emulating someone else.)**

□ 3. Is your router configured with the “no IP” directed-broadcast command? If not, for what purpose is IP directed-broadcast required?

□ a. Is source routing disabled on your router?

□ b. Has the “no IP” source-route been set on your router?

□ c. Does your router use automated features (such as Cisco’s quality of service — QoS) to protect hosts and links against certain floods?

### 2.1.2 Firewalls

□ 1. Have you disabled packet filtering to send packets that will exercise all routing rules through the firewall system

□ 2. **CDC strongly recommends the use of a "secure subnet architecture" or DMZ established with two or more firewalls. Does your security configuration include a DMZ with a second firewall for the protection of the NBS?**

□ 3. What firewall software are you using? On what hardware platform? Where is the firewall physically located (what building)?

□ 4. How often are firewall logs and scanner results reviewed? Does the review include the following activities?

□ a. Trigger packet filtering—Inject network traffic that is an appropriate sampling of all possible source and destination IP addresses, across all ports, and for all protocols

□ b. Ensure that packets are blocked (denied) as intended

□ c. Examine all the logged network traffic and verify that logging options associated with each packet-filtering rule are operating as intended

□ d. Examine all logged network traffic, and verify that alert options associated with each logging option send notices to the appropriate destination

### 2.1.3 Authentication Administration

□ 1. Has SSL encryption connection been deployed to access your site Web server? If so, have you also extended encryption connections from your Web server to applications?

□ 2. Who is your certificate authority for SSL certificates (your own certificate server, Verisign, Entrust, etc.)?

□ 3. How is positive identity binding established in the acquisition of certificates for access to your sensitive information resources? If you issue digital certificates directly to users, what is the process used to ensure the identity of the requestor?

□ 4. What kind of authentication services are currently implemented (NT Domain, X509 certification, LDAP, security token, etc.)?

□ 5. Do you plan to implement single sign-on login?

□ 6. Has the Information System Security Office (ISSO) developed and approved a method to control access to system tapes or disks?

□ 7. Has each individual user been assigned a unique user identification and password that has been randomly machine generated?

□ 8. Is there a process in place for requesting and approving system changes before they are made?

□ 9. Does the ISSO maintain and monitor a log of all system patches?

□ 10. How frequently are checks for weak accounts/passwords and mail vulnerabilities performed? Do these checks include:

□ a. No passwords

□ b. Default accounts

□ c. Predictable passwords

□ d. Crackable passwords

□ e. Old mail versions

□ f. Mail buffer overflows

□ g. Misconfigurations

□ h. Confirming roles and responsibilities of all system users

□ i. Account restrictions

□ j. Password strength

□ k. Access control

□ l. Workstation lockouts

□ m. Screen saver passwords

□ n. System monitoring settings

□ o. Audits (implemented and reviewed)

□ 11. Is all of the software (including the current version number) reflected in a site security policy?

□ 12. Is authenticity of the operating system software verified by comparing the registry or shipment number of the software package with that contained in record communications from the originator?

□ 13. Is proper documentation available for all software, and are all modules and interfaces described in detail?

□ 14. Is an inventory of all software maintained?

□ 15. Before operational use of any new system release, does the ISSO conduct sufficient testing to verify that the system meets the security requirements?

□ 16. Are new releases tested and debugged during dedicated time in a controlled environment?

□ 17. Are all software patches unique to the site tested by software personnel?

## 2.2 Intrusion Detection Checklist

Intrusion detection is most important for Internet NBS implementations. However, even Intranet only NBS implementations should include some intrusion detection and monitoring to protect against by unauthorized individuals who may manage to gain physical access to internal computers.

□ 1. Do the network systems have any intrusion detection or real-time monitoring software installed, and if so, are they host (server) or network intrusion?

□ 2. Are security enforcing components identified and can you provide a list of all components?

□ 3. Does the systems architecture documentation include graphics and successfully describe the architecture of the system? Does the documentation explain the interconnections that provide or support system functions?

□ a. Does the system architecture identify and describe the hardware configuration?

□ b. Does the system architecture identify and describe the software configuration?

□ c. Does the system architecture identify and describe all external connections?

□ d. Is a network configuration diagram available?

□ 4. Does the system maintain a domain for its own execution that protects it from external interface or tampering?

□ 5. Does the system or network connect to any other network or systems?

□ 6. Have all the potential backdoors to your network been closed (e.g., internal, external modems)? Include checks with backdoors and trojans for SubSeven and BackOrifice, and read the simple network management protocol (SNMP) for vulnerabilities.

□ 7. Are non-security-enforcing components identified whose failure or misuse could compromise security?

□ 8. Have you checked for request for protocol (RPC) service vulnerabilities, including

□ a. Vulnerable services

□ b. Buffer overflow

□ 9. Are announced/unannounced, monitoring/penetration vulnerability assessment processes or procedures in place?

□ 10. Are vulnerabilities and discrepancies analyzed to determine their susceptibility to exploitation?

□ 11. Are network analysis tools used to monitor the integrity of the system?

□ 12. If sensitive information is being transmitted, is it being protected by products that conform to Defense Encryption Standards (DES) in FIPS PUB 46-1 and FIPS PUB 140 or their successors?

□ 13. If DES products do not protect sensitive information being transmitted, has a waiver to these standards been granted pursuant to Section 3506(b) of Title 44 U.S. Code?

□ 14. Is the ISSO the focal point for all security matters for the IT systems assigned?

□ 15. Have the duties and responsibilities of the ISSO been defined in writing?

□ 16. Do the ISSO duties include the following:

□ a. Monitoring system activity (identification of the levels and types of data handled by this IS system, assignment of passwords, review of audit trails, etc.) to ensure compliance with security directives and procedures

□ b. Security oversight and monitoring of remote IS components or to ensure compliance with security requirements

□ c. Supervising, testing, and monitoring changes in the IT system affecting the IT activity posture, as appropriate

□ d. Implementing or overseeing the implementation of the Security and Training and Awareness Program

□ e. Ensuring that all IT security incidents or violations are investigated, documented, and reported to appropriate authorities

## 2.3 Web Server Checklist

□ 1. Does the Web server support HTTP and HTTPS? What other protocols are supported?

□ 2. If HTTPS is supported: is it enabled, and if so, what sites connect to the Web server?

□ 3. Is the Web server configured to support a 2-way certificate exchange with the NBS server?

□ 4. Has all software on the system been properly licensed?

□ 5. What are the port numbers for the application services?

□ 6. What kinds of remote access to your network are supported? How is security enforced for remote access? Are connection time-outs in place? Are all remote workstations or terminals uniquely identified when accessing the host (server)?

□ 7. Have the systems been scanned for vulnerabilities? If so, what tool(s) were used? Are scans done on a scheduled basis?

□ 8. If the systems have not been scanned for vulnerabilities, have manual checks been performed including: Windows NULL service data leaks, network file service (NFS) vulnerabilities, and Windows Registry vulnerabilities?

□ 9. Have Windows privilege access been checked for vulnerabilities?

□ 10. Does the Web system have a security architecture, and if so, does it implement the security policy and requirements?

□ 11. Who are the network, sever and database administrators and the security officers?

□ 12. Are the commercial off-the-shelf (COTS), Government off-the-shelf (GOTS), and internally developed products certified?

□ 13. Have the COTS or GOTS and internally developed products been evaluated for security vulnerabilities?

□ a. Have the Web products been checked for viruses, Y2K compliance, backdoors or trapdoors?

□ b. Is public domain software included in the products?

□ c. What programming languages were used to develop internally developed products (C, JAVA, Active-X, etc.)?

□ 14. Have any modifications been made to previously approved products?

□ a. If modifications have been made, have the modifications been evaluated for security vulnerabilities and re-certified?

□ 15. Are configuration management (CM) procedures in place for additions of new software, updated software, and maintenance of software?

□ 16. Does the operating system meet the requirement for ongoing security auditing? For example:

□ a. Is industry standard security logging activated? Are logs reviewed in detail at least weekly? Are intrusion detection tools in use? How are intrusion event alerts handled?

□ b. Are the audit requirements defined and documented? Is an audit checklist or audit support software in use?

□ c. What are the backup, archiving, retention and destruction policies for audit logs?

□ d. Some audit logs may contain personal privacy information. How are those logs identified and protected? How are audit logs protected from unauthorized access or destruction?

□ 17. How well does your web operating system meet your requirements for data confidentiality?

## 2.4 System Fault Tolerance Checklist

□ 1. What contingency plan will be in existence for the NBS? If there is no existing plan how will a plan be established and by whom?

□ 2. Does the contingency plan address (at a minimum) the following:

□ a. Backup procedures to conduct essential IS operational tasks after a disruption to the primary IS facility

□ b. Duplicate system tapes, startup tapes/decks, database save tapes, and application program tapes unique to the site to be maintained in a secure location removed from the central computer facility

□ c. Recovery procedures to permit rapid restoration of the IS facility following physical destruction, major damage, or loss of data

□ 3. Is a backup copy of all applications software, operating system and system utilities maintained? Are backup copies stored offsite? How frequently are backup copies made? Do systems critical to NBS provide for transaction logging?

□ 4. Are the backup copies protected in a manner similar to the original copies including control of electronic access and physical security of media?

□ 5. Are CM procedures in place and change controls documented? If not do you have current plans to establish such procedures?

□ a. Is the authenticity of the operating system or executive software verified by comparing the registry or shipment number of the software package with that contained in record communications from the originator?

□ b. Before operational use of any new system release, does the ISSO or an equivalent authority conduct sufficient testing to verify that the system meets the documented and approved security specifications?

□ c. Does the ISSO or CM Review Board maintain a system baseline and backup?

□ 6. How are system modifications reflected in the security policies and what procedures in place to keep the security system configuration current? How is compliance with these policies monitored?

## 3.0 Security Policy and Procedures Checklists

A minimum set of security management control policies and procedures is required to support the security measures you establish. These policies and procedures will be of little use if they are not published and available to all users in a timely fashion.

□ 1. Who is responsible for defining and publishing security policies and procedures? How is their work reviewed and validated? How frequently are reviews and audits of security policies undertaken?

□ 2. Publication of policies governing the appropriate use and access to information resources is critical. Are appropriate use policies published and available to all users? Do they address at least:

□ a. Requirements for the authentication of users

□ b. Control of access to systems and data resources including network, workstation, and server platforms as well as software, hardware and facilities physical security.

□ c. Use, publication and redistribution of data

□ d. Procedures for authorization and management of encryption of data

□ e. Provisions for monitoring of data, systems, and employee activities

□ f. Procedure, chains of authority and methods/formats for reporting violations

□ 3. How are data management policies established, published and available to all users? Do they address at least:

□ a. Ownership of and responsibility for data including protection of privacy.

□ b. Preservation of data including version management, backup and recovery.

□ c. Life-cycle support of data (retention and expiration)

□ 4. Policies and procedures must be communicated to those who are expected to abide by them. Are server and operations policies published and available to all users? How do they address:

□ a. Regular review of new security alerts relating to operating systems and other software

□ b. Procedures for reviewing and approving changes in place and documented.

□ 5. On-going audit and review of security precautions is critical. What procedures have you defined for security review of new applications?

□ 6. What mechanisms do you have in place to ensure that security changes to Internet and intranet resources (firewall, router, etc.) requested to support new applications or implementations do not compromise existing applications?

## 4.0 Security Training Checklists

Both end users and information systems personnel must be kept up to date on policies, procedures, and the latest innovations. Training should be ongoing.

□ 1. How is user security awareness training accomplished?

□ 2. How are Information Systems employees informed about changes to policies and procedures? How are new employees indoctrinated?