U.S. Customs and
Border Protection

Attachment O

Vulnerability Management Program

HB 1400-05D
Information Systems Security Policies and Procedures Handbook

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	July 27, 2009	Initial CBP 1400-05D release based solely on DHS 4300A, Version 6.1.1, attachment. There are no substantive differences between this CBP attachment and its source DHS attachment. This attachment is included as part of the CBP 1400-05D handbook suite to enable the CBP user to be able to access all IT security policies (DHS as well as CBP specific) at one location.
2.0	December 21, 2010	No changes.

CONTENTS

1.0 INTRODUCTION....1
1.1 Purpose....1
1.2 Scope....1
1.3 Authorities....1

2.0 INFORMATION SECURITY VULNERABILITY MANAGEMENT (ISVM) PROGRAM 1
2.1 Goals 1
2.2 ISVM Program Overview....1
2.2.1 Monitoring 3
2.2.2 Notification 3
2.2.3 Remediation....3
2.2.4 Compliance 3
2.2.5 Reporting....4
2.3 Vulnerability Assessment Notification, Approval Requirements....4
2.3.1 Request and Approval Process....4
2.3.2 Ad-hoc Assessments 4
2.4 Threats....4

3.0 ASSESSMENT PROCESS....4
3.1.1 Phase 1: Planning....5
3.1.2 Phase II: Discovery....5
3.1.3 Phase III: Attack 6
3.1.4 Phase IV: Reporting....6
3.2 Vulnerability Assessment Weekly Reporting....6

4.0 ASSESSMENT TYPES 7
4.1 Internal Assessments....7
4.1.2 External Assessments....8

5.0 INFORMATION SECURITY VULNERABILITY MANAGEMENT (ISVM) NOTICES....8
5.1 DHS CSIRC Responsibilities 10
5.2 Component CSIRC Responsibilities....10

Appendix O1—DHS Vulnerability Assessment After-Action Report Template

Appendix O2—ISVM Notice Categories

Appendix O3—ISVM Notice Template

1.0 INTRODUCTION

1.1 Purpose

Attachment O, *1400-05D IT Security Policy and Procedures Handbook*, documents the DHS Information Security Vulnerability Management (ISVM) program requirements, procedures and guidance for all Department of Homeland Security (DHS) Components, including CBP. It includes procedures for participation and management of the program as well as reporting requirements.

1.2 Scope

These procedures apply to all DHS *For Official Use Only* (FOUO) systems.

1.3 Authorities

A. Federal Information Security Act (FISMA) of 2002, PL 107-347, Title III

B. Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources

C. NIST Special Publication 800-42, Guideline on Network Security Testing, October 2003

D. NIST Special Publication 800-53, Revision 2, Recommended Security Controls for Federal Information Systems, December 2007

E. Department of Homeland Security Management Directive (MD) 4300, IT System Security

F. Department of Homeland Security (DHS) 4300A, *Sensitive Systems Handbook*, Attachment O- Vulnerability Management Program

2.0 INFORMATION SECURITY VULNERABILITY MANAGEMENT (ISVM) PROGRAM

2.1 Goals

The goal of the DHS Information Security Vulnerability Management (ISVM) program is to proactively increase security situational awareness of, and minimize risks to, DHS information systems, through a comprehensive vulnerability alert, assessment, remediation and reporting process. The DHS ISVM is a Department-wide program intended to ensure an effective, continuous process to manage computer security vulnerabilities, risks and threats. Such a program must provide assurance of comprehensive coverage, proper notification, approval, and coordination across the DHS enterprise. The ISVM allows DHS and Component Security Operations Centers (SOCs) to effectively identify computer security vulnerabilities and track mitigation efforts to resolution.

2.2 ISVM Program Overview

The ISVM program employs a hierarchical approach that allows Components to choose whether to use their internal capabilities to establish Component vulnerability management programs consistent with DHS policy or, at their discretion, choose to outsource this task to the DHS SOC via a Memorandum of Agreement (MOA).

Vulnerability assessment (VA) scans must be performed to inspect 100% of DHS and Component systems at least annually. In all cases, detailed VA scan schedules and results must be provided to the DHS SOC in order to create DHS OCIO enterprise-wide security situational awareness of assets and risks as mandated by FISMA. A subset of Component systems will be selected for vulnerability assessment scans that are more frequent, more thorough, and/or application-specific. A smaller number of Component systems may be selected for annual penetration testing, at the discretion of the DHS CIO. Criteria for selecting Component systems for additional testing include mission/organization criticality or increased risk resulting from the system's location or visibility.

Vulnerability management responsibility rests with Component Chief Information Security Officers (CISOs)/Information System Security Managers (ISSMs). In addition to assessments conducted by Components, the DHS SOC, under the direction of the DHS Chief Information Officer (CIO), may conduct ongoing assessments of any DHS system at any time given sufficient coordination and approval.

The five phases of the Information Security Vulnerability Management Program include:

1. Monitoring
2. Notification
3. Remediation
4. Compliance
5. Reporting

The ISVM consists of a five phase closed loop vulnerability management process, as depicted in Figure O-1.

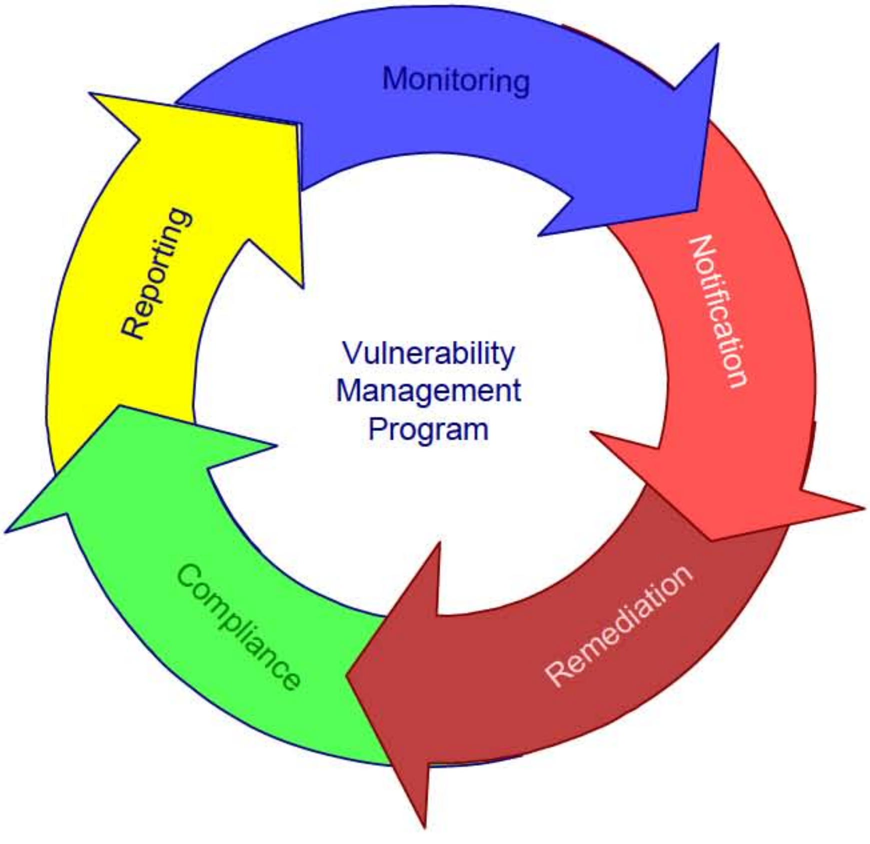


Figure O-1: Information Security Vulnerability Management Program

2.2.1 Monitoring

The monitoring phase is a continuous process whereby the DHS SOC, Component SOCs, ISSMs, and ISSOs ensure that their systems are continuously monitored to include the latest patch levels and comply with configuration guidance. This is performed by reviewing current vendor patch notifications, security configuration best practices, security architecture guidance, and emerging threats and vulnerabilities.

2.2.2 Notification

Notification is the process whereby the DHS SOC reviews emerging threat and vulnerability notifications as part of the monitoring phase, and creates risk-based ISVM notifications whenever new vulnerabilities are discovered or new threats emerge. The DHS SOC issues ISVM notifications to Components when a risk-based decision dictates the need for a Department-wide notification. Component CISOs/ISSMs are required to acknowledge receipt of the ISVM notification.

Component SOCs may also issue notifications to those within their Watch Areas, if they deem that a notification is necessary. This may happen when a Component operates within a specific environment that does not necessitate a DHS-wide ISVM notification.

2.2.3 Remediation

Components are required to comply with the ISVM notification, or complete the waiver request information on the DHS SOC Online Portal. Vulnerability remediation responsibility rests upon the system owner. System owners will work with their ISSOs and CISOs/ISSMs to establish remediation priorities. CISOs/ISSMs should carefully consider the risk and impact of the vulnerability when establishing remediation priorities.

The DHS SOC does not grant waivers for patching systems, this role is the responsibility of the system DAA. The information regarding the waivers is collected for oversight and situational awareness within DHS.

2.2.4 Compliance

Compliance is a mechanism to independently verify systems comply with ISVM notices, patch notifications from vendors, security configuration guidance, and the DHS Security Architecture. Compliance is verified through Vulnerability Assessments (VA) conducted at least annually on all DHS systems.

2.2.4.1 Component Vulnerability Assessments

Components may perform annual vulnerability assessments and will develop annual vulnerability assessment schedules that include complete coverage for all systems within each calendar year. The schedules must be provided to the DHS SOC and may be updated as often as necessary. Schedules, updates, assessment, and remediation results will be provided to the DHS SOC as they become available.

2.2.5 Reporting

Reporting is the process to help identify and validate the number of systems that comply with DHS security guidance. This reporting directly impacts the Department's FISMA score and enables DHS leadership to view system compliance capability with the DHS security guidance.

2.3 Vulnerability Assessment Notification, Approval Requirements

Assessments within DHS Components, as well as broader DHS vulnerability assessments, must follow a standard request, notification, and approval process. This standardized process reduces the possibility that assessment activity will be misinterpreted as malicious and better ensures that it is not conducted without appropriate approval.

2.3.1 Request and Approval Process

Assessments conducted by Components will be performed in accordance with the Components' internal request procedures and must be approved by the Component ISSM.

Components may request that the DHS SOC Vulnerability Assessment Team (VAT) team perform a vulnerability assessment or penetration test. Components submit this request via the DHS SOC Online Portal at https://soconline.dhs.gov (accessible only via the DHS Intranet).

The SOC will coordinate with the appropriate ISSM(s) and other entities, as required, based on the type of assessment being conducted. Coordination will be established at a kick-off meeting. The kick-off meeting will be a brief forum for individuals involved to confirm and answer any questions involving the exercise. The DHS SOC will provide updates to Component personnel as necessary, notify the Component CISO/ISSM when all assessment-related activity is complete, and schedule an out brief meeting when reports are complete.

2.3.2 Ad-hoc Assessments

The DHS SOC may conduct scans of any DHS asset at the direction of the DHS CIO. No prior approval or notification is required for this type of assessment.

2.4 Threats

Various threats seek to actively exploit vulnerabilities in DHS systems. In order to effectively conduct its missions and maintain public confidence, DHS must ensure that its information systems are resilient to as many active threats as possible. Modern information systems face a number of threats both within and from outside their boundaries. DHS will take necessary measures to track the latest threat information and recommend mitigations as part of its vulnerability management process.

3.0 ASSESSMENT PROCESS

As depicted in Figure O-2, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-42, *Guideline on Network Security Testing*, describes vulnerability assessment as a four-phase process – Planning, Discovery, Attack, and Reporting.

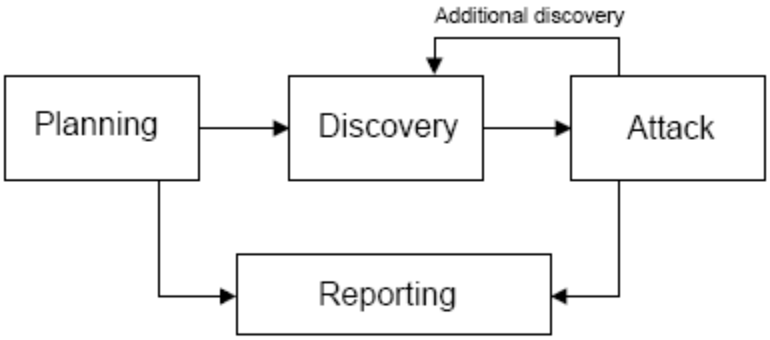


Figure O-2: Vulnerability Assessment Process

3.1.1 Phase 1: Planning

The planning phase sets the foundation for each assessment. Rules are identified, management approval is finalized, testing goals are set and the timeline for submitting the final report is established during this phase. No actual testing occurs.

The Vulnerability Assessment Team (VAT) gathers information about the system(s) and/or network(s) to be assessed through a variety of sources, including:

- Review of system documentation and Certification and Accreditation (C&A) documents
- Interviews with Information System Security Managers (ISSM), Information System Security Officers (ISSO), system owners, users, and other stakeholders
- Review of open source information

The VAT will verify all relevant Internet protocol (IP) addresses and develop a test plan, which will guide them through the remaining phases. The plan will include a test schedule and a list of tools and techniques that will be used to identify vulnerabilities. This may involve the use of proprietary or open source Commercial Off The Shelf (COTS) or Government Off The Shelf (GOTS) products. Any tools used for this purpose must be approved in advance by the ISSM(s) of the Component whose systems are being scanned.

3.1.2 Phase II: Discovery

Testing begins with the discovery phase. Services, applications, and operating systems are scanned and the results are compared against vulnerability databases.

Testing may be conducted locally or remotely. Additionally the VAT may enumerate the network infrastructure and analyze any filtering or routing that may contribute to evaluating the overall security posture. Other techniques used to identify vulnerabilities may include:

- Domain Name System (DNS) interrogation
- Search of the target server(s)
- Search of Lightweight Directory Access Protocol (LDAP) server(s)
- Packet capture
- NetBIOS enumeration

- Banner grabbing

3.1.3 Phase III: Attack

The attack phase is where previously identified vulnerabilities are verified by attempting to exploit them. A successful attack results in the vulnerability being verified and safeguards identified to mitigate any security exposures. The objective is not to gain the maximum level of access, but to allow the VAT to learn more about the targeted network and its potential vulnerabilities. Additional analysis is required to determine the true level of risk.

Some systems require more detailed analysis. Under these circumstances, a penetration test (Pen Test), a method of evaluating a system's security by actively simulating a malicious attack, may be conducted. This type of assessment can be very time consuming and costly and is, therefore, generally reserved for testing specific high value targets.

Whenever penetration testing is conducted, the request and approval documentation must provide specific instructions and authorization for the types and extent of penetration to be conducted, reporting criteria, coordination, notification requirements, and cessation or back-out criteria. No penetration testing will be conducted without prior approval from the ISSM(s) of the system(s) being tested.

3.1.4 Phase IV: Reporting

Upon completion of Phases I-II and if requested Phase III, the VAT will analyze the results and develop a final report to be delivered to the CISO/ISSM and system owner within the timeframe established during Phase I. Vulnerability assessment reports will contain the elements listed in Appendix O1. The reporting phase provides system owners and CISOs/ISSMs with the results of Phases II and III and includes an assessment of their impact and recommendations for mitigation. Vulnerabilities are identified in terms of criticality, allowing management to prioritize and systematically eliminate or mitigate vulnerabilities. Reports will list specific vulnerabilities, recommended mitigation, and a recommended timeframe for each.

System owners will work with their ISSOs and CISOs/ISSMs to correct vulnerabilities within the recommended timeframe. Those vulnerabilities that cannot be corrected within this period will be tracked through the Plan of Actions and Milestones (POA&M) process.

3.2 Vulnerability Assessment Weekly Reporting

Weekly reporting will be conducted and incorporated into the current DHS SOC reporting process. The vulnerability assessment portion will include:

- Addresses/systems assessed
- Man-hours expended
- Critical Vulnerabilities detected, corrected, and remaining open
- Total Verified Vulnerabilities found

4.0 ASSESSMENT TYPES

The DHS VAT provides several different types of assessments to fulfill a variety of organizational requirements.

4.1 Internal Assessments

Vulnerability assessments (VA) are considered internal if they are conducted entirely within the boundaries of the DHS network. Internal assessments are conducted according to a schedule that ensures annual coverage for all internal assets. The intended focus of VA is to rapidly discover and identify vulnerabilities within the specified network region. Every effort is made to minimize the possibility of interruptions to operational information assets. As is typical methodology for vulnerability assessment, the VAT follows strict signed rules of engagement to avoid loss of data or availability during these exercises, including when granted prior approval to conduct Phase III penetration testing. The following rules apply to all DHS vulnerability assessments:

- Denial-of-service attacks are not performed.
- Backdoors, malware, viruses, corrupted data, and/or Trojans are not installed.
- Tools and techniques that require the least amount of bandwidth possible are used to better ensure minimal impact on network traffic.
- Untested tools or techniques are not used. All tools and techniques are reviewed and tested in a lab environment before they are used.
- No software, scripts, or code is uploaded/installed during the vulnerability assessment.

4.1.1.1 Conducting the assessment

Internal vulnerability assessments are conducted in accordance with a mutually agreed upon vulnerability assessment schedule. However, there will be situations in which unscheduled assessments, with little or no notice, will be necessary. During these unscheduled assessments, the DHS VAT will take proactive steps to ensure that alerts generated by the assessment activity are stopped at the appropriate level.

Internal vulnerability assessments, both scheduled and unscheduled, will contain elements of the first two vulnerability assessment phases. Phase III penetration testing will only be conducted when deemed necessary, approved by the approval authority, and clearly defined regarding scope and techniques to be used.

4.1.1.2 Reporting

A final report, detailing the findings, will be generated and provided to the system owner and ISSM. The report will include overview of the findings and detailed information concerning vulnerabilities, their criticality, and recommendations for remediation. Vulnerability assessment reports will contain the required minimum elements identified in Appendix O1. Copies of all reports will be provided to the DHS SOC.

4.1.2 External Assessments

Vulnerability assessments are considered external if they are targeted at points of entry to the DHS network from outside the DHS network perimeter. External assessments may include security testing at DHS Internet connections, remote access and dial-up connections, mail gateways, interagency connections, partner connections (contractors, universities, etc.), wireless connections, and other points of entry to the DHS network. This type of assessment may also include searches for network back doors and may incorporate elements of social engineering when pre-approved and appropriate.

The intended focus of the external vulnerability assessment is to rapidly discover and identify vulnerabilities that may result in compromise of DHS information or assets. Every effort will be made to minimize interruption of services.

4.1.2.1 Conducting the Assessment

External vulnerability assessments are normally conducted by the DHS. There may be times when external vulnerability assessments are conducted on an unscheduled basis with little or no notice. During these unscheduled, no-notice assessments, the DHS SOC may restrict advance notification to a limited number of persons to better ensure success of the unscheduled assessment. The DHS VAT will take appropriate steps to ensure that alerts generated by the assessment activity are stopped at the appropriate level.

4.1.2.2 Reporting

A final report, detailing the findings will be provided to the appropriate system owner, CISO/ISSM or other approval authority. The report will include detailed information concerning vulnerabilities and mitigation recommendations. Vulnerability assessment reports will contain the required minimum elements identified in Appendix O1. Copies of all reports will be provided to the DHS SOC.

5.0 INFORMATION SECURITY VULNERABILITY MANAGEMENT (ISVM) NOTICES

The DHS CSIRC ISVM team will conduct daily monitoring to stay abreast of current vulnerabilities, risks and threats to DHS information systems and data. The ISVM team will provide notification and recommendations to Components via ISVM notices (and other avenues as circumstances require). These notices will take one of three forms.

- Information Security Vulnerability Alert (ISVA)
- Information Security Vulnerability Bulletin (ISVB)
- Technical Advisory (TA)

The characteristics of the vulnerabilities, messages, and the required Component actions are outlined in the following table.

	ISVA	ISVB	TA
Risk	Severe	Medium	Low
Acknowledgement	Yes	Yes	No

	ISVA	**ISVB**	**TA**
Compliance*	Yes	Yes	Yes
Compliance Confirmation	Yes	Yes	No
* Compliance is required if affected systems are present within the Component			

Additional descriptions for ISVM categories and thresholds are defined in Appendix O2, ISVM Notice Categories.

Anyone within DHS may request to be added to the ISVM distribution list. Those wishing to be added must provide a DHS email address and obtain management approval. ISVMs contain sensitive, "For Official Use Only" information and must be handled in accordance with relevant policy for protection of such information. ISVM notices must not be forwarded to non-DHS email accounts. ISVM notices also must not be forwarded to persons outside of the DHS information security support community, without prior approval of an authorized DHS official.

Although ISVM messages can be sent to anyone, *only Component CISOs/ISSMs* or their designated representatives may acknowledge receipt of messages, report compliance with requirements or notify the granting of waivers.

ISVM messages will have the same general format and will contain the following sections, as applicable:

- Message number
- Version
- Related Common Vulnerabilities and Exposures (CVE) numbers
- Release date
- Subject
- Executive summary
- Requirements
  - Acknowledgment (yes/no)
  - Acknowledge by date
  - Compliance (yes/no)
  - Compliance by Date
  - Reporting Instructions
- Affected systems
- Details
- References
- Required actions
- Recommended actions

- Contact information
- Revision information

See the ISVM message template in Appendix O3.

Components should report compliance with the ISVM message within the specified timeframe. Components unable to meet the designated compliance timeframe must submit documentation of a waiver request via the DHS SOC Online Portal at https://soconline.dhs.gov (accessible only via the DHS Intranet).

Waivers are granted by the system Designated Accrediting Authority (DAA). Requests must specify the specific corrective action that cannot be taken, list the number of affected systems by type, explain why the action cannot be completed, and include the mitigating steps taken, and a timeline/plan for bringing the systems into compliance. Waiver requests should be submitted as soon as the need is identified.

Please note that the DHS SOC collects and maintains information regarding ISVM waivers in order to maintain oversight and situational awareness. Responsibility for approving waiver requests and granting of waivers rests with the system DAA.

Correspondence regarding ISVM messages should be sent via email to dhs.soc@dhs.gov.

The DHS CSIRC will forward advisories from US-CERT, as appropriate, and ensure that each Component is alerted. In cases where the alert, advisory or warning is time critical, the DHS CSIRC may also inform each DHS Component CIO and POC via telephone. The Component POCs will be asked to reply to the DHS CSIRC within a specified time period for instances requiring response to external organizations.

5.1 DHS CSIRC Responsibilities

The DHS CSIRC is responsible for providing timely dissemination of ISVM advisories and vulnerabilities to the designated points of contacts within each Component CSIRC. ISVM advisories and vulnerabilities are made available to the Component CSIRCs through the Web portal.

The DHS CSIRC also serves as the first point of contact for any Component researching an anomaly. The DHS CSIRC is the primary interface of the DHS for third party organization reporting for security incidents, vulnerabilities, and countermeasures released. The DHS CSIRC coordinates with third parties to answer questions a Component may have.

5.2 Component CSIRC Responsibilities

The Component CSIRC is responsible for distributing ISVM advisories and vulnerabilities received from the DHS CSIRC either through electronic mail or through telephone or pager calls to the appropriate individuals within the Component (e.g., network operations centers, system administrators, Information System Security Officers [ISSOs]).

Appendix O1
DHS Vulnerability Assessment After-action Report Template

DHS Vulnerability Assessment After-action Report Template

This section provides the minimum requirement for vulnerability assessment after-action reports. Reports may include more detail than identified below, but not less. Reports in the following format are due to the DHS SOC no later than five working days after completion of the assessment.

Report Title

1. Executive Summary
    a. Organization Performing Assessment
2. Background
    a. Purpose
    b. Scope
        i. POC listing with contact info
        ii. Date/Time
        iii. Target Network
3. Methodology
    a. Reconnaissance
    b. Scanning
    c. Penetration
    d. Reporting
4. Findings and Recommendations
    a. Vulnerability Rating
        i. DHS Critical Vulnerabilities
        ii. Other Critical Vulnerabilities
        iii. Other Relevant Vulnerabilities
5. Conclusions

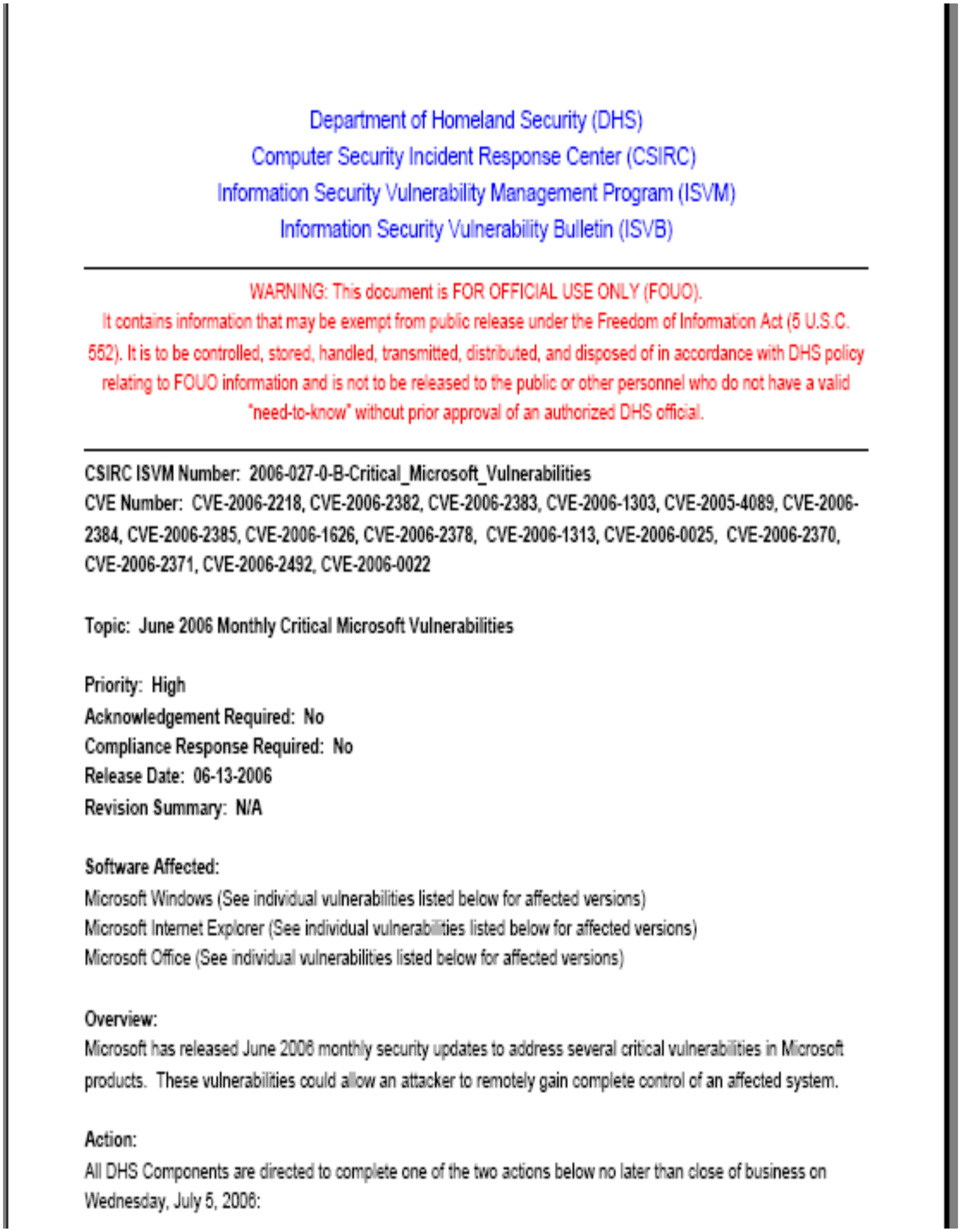
Appendix O2
Information Security Vulnerability Management (ISVM) Notice Categories

- ISVA (Information Security Vulnerability Alert)
  - Significant risk vulnerability (risk is calculated by considering likelihood of exploitation, potential for damage, and number or importance of affected systems)
  - Immediate threat to DHS infrastructure, data and/or mission
  - Acknowledgement required
  - Compliance action (or waiver) required, usually within 1 week
  - Confirmation of compliance (or waiver) required, usually within 1 week

- ISVB (Information Security Vulnerability Bulletin)
  - Medium risk vulnerability
  - Possibility that threat may increase
  - Acknowledgement required
  - Compliance action (or waiver) required, usually within 2 weeks
  - Confirmation of compliance (or waiver) required, usually within 2 weeks

- TA (Technical Advisory)
  - Low risk vulnerability
  - Potential escalation unlikely
  - Acknowledgement is not required
  - Compliance action may be required
  - Confirmation of compliance is not required

Appendix O3
ISVM Message Template



Department of Homeland Security (DHS)
Computer Security Incident Response Center (CSIRC)
Information Security Vulnerability Management Program (ISVM)
Information Security Vulnerability Bulletin (ISVB)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO).
It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

CSIRC ISVM Number: 2006-027-0-B-Critical_Microsoft_Vulnerabilities
CVE Number: CVE-2006-2218, CVE-2006-2382, CVE-2006-2383, CVE-2006-1303, CVE-2005-4089, CVE-2006-2384, CVE-2006-2385, CVE-2006-1626, CVE-2006-2378, CVE-2006-1313, CVE-2006-0025, CVE-2006-2370, CVE-2006-2371, CVE-2006-2492, CVE-2006-0022

Topic: June 2006 Monthly Critical Microsoft Vulnerabilities

Priority: High
Acknowledgement Required: No
Compliance Response Required: No
Release Date: 06-13-2006
Revision Summary: N/A

Software Affected:
Microsoft Windows (See individual vulnerabilities listed below for affected versions)
Microsoft Internet Explorer (See individual vulnerabilities listed below for affected versions)
Microsoft Office (See individual vulnerabilities listed below for affected versions)

Overview:
Microsoft has released June 2006 monthly security updates to address several critical vulnerabilities in Microsoft products. These vulnerabilities could allow an attacker to remotely gain complete control of an affected system.

Action:
All DHS Components are directed to complete one of the two actions below no later than close of business on Wednesday, July 5, 2006: