Information Assurance Vulnerability Alert
DISA Internal Process and System

Jacqueline Price Snouffer
jackie.snouffer@ritchie.disa.mil
(7 17) 267-9997
9 February 1999
Form SF298 Citation Data

<table>
<thead>
<tr>
<th>Report Date</th>
<th>Report Type</th>
<th>Dates Covered (from... to)</th>
</tr>
</thead>
<tbody>
<tr>
<td>09021999</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title and Subtitle</th>
<th>Contract or Grant Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Assurance Vulnerability Alert DISA Internal Process and System</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authors</th>
<th>Project Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Task Number</td>
</tr>
<tr>
<td></td>
<td>Work Unit Number</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Performing Organization Name(s) and Address(es)</th>
<th>Performing Organization Number(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISA</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sponsoring/Monitoring Agency Name(s) and Address(es)</th>
<th>Monitoring Agency Acronym</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Monitoring Agency Report Number(s)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Distribution/Availability Statement</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved for public release, distribution unlimited</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Abstract</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Subject Terms</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;IATAC COLLECTION&quot;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Document Classification</th>
<th>Classification of SF298</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Classification of Abstract</th>
<th>Limitation of Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unlimited</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Pages</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td></td>
</tr>
</tbody>
</table>

Supplementary Notes

Abstract

Subject Terms
"IATAC COLLECTION"

Document Classification
unclassified

Classification of Abstract
unclassified

Number of Pages
22
**Abstract**

This briefing outlines DISA's internal procedure for tracking IAVAs. It discusses the policy, procedures, organizations responsible for tracking the IAVAs, and the security features of the program.

**Subject Terms**

DISA, vulnerability
DOD has mandated that all C/S/A develop a methodology for ensuring:

- Vulnerability alert notifications are received by System Administrators
- Vulnerabilities are corrected within 30 days
- Periodic/Randdom validation of system status
Vulnerability Compliance Tracking System

- Provide the ability to quickly notify and receive acknowledgement from subordinates of an IAVA

- Assess the impact of a vulnerability on the infrastructure

- Monitor status and closure of vulnerabilities

- Provide reporting to DoD of compliance
Vulnerability Compliance Tracking System

1. Alert Notice
   - Assist
   - VCTS Web Page
   - SA/ISSM/CC

2. Verify Receipt
   - SA
   - VCTS Web Page

3. Get Patch
   - SA
   - VCTS Web Page
   - ASSIST Web Page

4. Log Status Updates, Request Waiver
   - SA
   - VCTS Web Page

5. Report DISA Compliance
   - VCTS Web Page
   - IAVA

Capabilities for
** System Registration
** System Administrator Updates and Permissions
VCTS Security Features

- NIPRNET/SIPRNET
- PKI Server
- Certificate
- 128 Bit SSL Encryption
  - Userid
  - Password
  - Data
  - IP Filtering
- Proxy Server
- NTFS Permissions
- SQL Server Permissions
- Encrypted Data
- Daily Backups
- Monitoring
Other Agency Use of VCTS

- Host on platform with DISA
  - Data segregated with strict access control
  - Costs to be negotiated

- POC
  - Danette Wile
  - 717-267-9933
  - wiled@ritchie.disa.mil
BACKGROUND
VCTS Capabilities

- Reporting/Oversight by ISSMs and Xos

- Update of SA/User information

- Registration/Update of Systems

- Delegation of browse & update to other SAs

- Automatic feed to IAVA of DISA’s posture
Vulnerability Compliance Tracking System (VCTS) Capabilities

- Notification of alert to registered users based on function
- Acknowledgement of receipt by system
- Process for requesting waivers
- Tracking of closure/posture of vulnerabilities
VCTS Registration Process

1. DISA Form 41
2. FAX
3. RSA Chambersburg
   - Create User’s NT Account
   - Load IP Address
   - Create User Profile
   - Prepare User Package
   - 5 Days or Less
4. Return Receipt via FAX
5. User Account Activated within 24 hours

DMC Chambersburg fax:
717-267-9055
DSN: 570

FEDEX 1 day

IAVA-VCTS
Message Dissemination

ASSIST

Post Alert on Web Site

EMAIL

D25, COE, D331, DISANET, NCS, NIPR/SIPRNET

EMAIL

VCTS

EMAIL

DISA POC (CIO)
Technical Channels
Command Channels
Registered within VCTS

DISA SA must report Vulnerability Alert receipt within 5 days.

C/S/A

Receipt counts are kept by system so that only one SA from each system needs to report for all systems affected.
Walver Process

1. SA Requests Waiver

2. Chain of ISSMs Notified via EMAIL for Approval

3. DAA Notified via EMAIL for Approval/Disapproval

4. ISSMs/SA Notified via Email of Decision

Steps 2-4 not automated at this time
User Types

- **XO**
  - Receive all IAVA Alerts
  - Organizational view of the data
  - Notified when waiver has been requested

- **ISSM**
  - Receive all IAVA Alerts
  - Organizational view of the data
  - Approves waiver prior to DAA adjudication
User Types

- System/Network Administrators
  - Receives only those bulletins for systems they have registered or have been given update authority for
  - Requests waiver
  - Cannot view system data that they have not been given explicit permission to
Current Reports Available

- **ISSM/XO**
  - Compliance Summary Report by Vulnerability (VM02)
  - Active Users by Organization (VM03)
  - Registered Systems by Organization (VM04)
  - Waiver Summary Spreadsheet (VM08)

- **SA/ISSM/XO**
  - Compliance/Acknowledgement Report by System (VSO 1)
  - Compliance/Acknowledgement Report by Vulnerability (VS02)
V 1.0 Outstanding Capabilities

• Complete Reporting
  – VS05/06 - Acknowledgement Report by User/System
    • By Organization/Site
    • By Alert
    • 1 March 1999

• Interim Waiver Process
  – CIO will grant/deny waivers regardless of accредitor
  – CIO will grant/deny waiver, indicate expiration date, and provide pertinent comments
  – Available 25 February 1999
V 2.0 Enhancements

- Link to Accredited System/Major Program
  - Allow for oversight by Program Management Office
  - Allow for Waiver Request/Granting for entire Program
  - Allow Email by PMO to SA(s)
  - Multiple accreditor based on system/program
  - Allow Accreditor to review site and system status
  - Allow Accreditor to review asset/component information
  - Cross Organizational browsing at program level
V 2.0 Enhancements

- Fully automate waiver process
  - Through ISSM/Program/Technical/Adjudication Chain
  - Process for Major Programs to be determined by Program
  - Multiple DAAs
  - Ability to establish different waiver processes depending on program or system

- Specifications out for comment on 1 March 1999
**V 2.x Requested Enhancements**

- **Status Information**
  - Update status after completion
  - Allow browse by XO, ISSM, PMO, CIO
  - Provide list of N/A reasons

- Allow ISSM to enter Organizational Comment

- **Acknowledgement**
  - Unacknowledge Receipt
  - Confirm Acknowledgement
V 2.x Requested Enhancements

- Subscription to bulletins
  - ISSM to give permission to a system within their organization to any registered SA
  - Supporting reports for new functionality