When this document is printed, the document needs to be stamped top and bottom with the appropriate classification.

VL05 - Checklist Report

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:
Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

Checklist: Sun Ray 4 Policy

Vulnerability Key: V0016397
STIG ID: SUN0010
Release Number: 4
Status: Active
Short Name: No up-to-date documentation or diagrams
Long Name: There is no up-to-date documentation or diagrams of the Sun Ray infrastructure.
IA Controls: DCSW-1 SW Baseline
Categories: 12.9 Documentation
Effective Date: 09 Sep 2008

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Sun Ray 4 Policy (Target: Sun Ray 4 Policy)
Policy: All Policies
MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

STIG ID: SUN0010
Severity: Category II

Long Name: There is no up-to-date documentation or diagrams of the Sun Ray infrastructure.

Vulnerability Discussion: Without current and accurate documentation, any changes to the Sun Ray infrastructure may jeopardize the network's integrity. To assist in the management, auditing, and security of the network, facility drawings and topology maps are a necessity. Topology maps and documentation are important because they show the overall layout of the network infrastructure and where devices are physically located. They also show the relationship and inter-connectivity between devices and where possible intrusive attacks could take place. If an incident were to occur, the lack of documentation would impact the ability to respond. Additionally, documentation along with diagrams of the network topology are required to be submitted to the Connection Approval Process (CAP) for approval to connect to the NIPRNet or SIPRNet.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: SUN0010 (Manual)

Request a copy of all the Sun Ray infrastructure documentation. Documentation must include all routers, switches, servers (Solaris, Windows), applications (such as Citrix XenApp and Sun Ray Software), Sun Ray Desktop Units, IP addresses, and any third party applications. If the documentation does not include all of these components, this is a finding.

Fixes: SUN0010 (Manual)

Develop up-to-date documentation for the Sun Ray infrastructure.

Vulnerability Key: V0016400
STIG ID: SUN0060
Release Number: 2
Status: Active
Short Name: User Registration process not clearly documented
Long Name: User Registration process is not clearly documented.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 09 Sep 2008

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Sun Ray 4 Policy (Target: Sun Ray 4 Policy)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

STIG ID: SUN0060
Severity: Category III
Long Name: User Registration process is not clearly documented.
Vulnerability Discussion: Without proper user registration documentation, users and system administrators may not register users in the Sun Ray system properly and potentially grant users more privileges than necessary.
Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: SUN0060 (Manual)

Request a copy of the user registration documentation from the IAO/SA. Review the document for step by step procedures in registering users in the Sun Ray System.

Fixes: SUN0060 (Manual)

Develop Sun Ray system user registration documentation.

Vulnerability Key: V0016409
STIG ID: SUN0100
Release Number: 3
Status: Active
Short Name: IAO/SA not receiving Security sec and patch info
Long Name: The IAO/SA is not receiving Sun Ray security and patch notifications.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 3.1 Security Patches
3.2 Operational / PM Patches
Effective Date: 09 Sep 2008

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Sun Ray 4 Policy (Target: Sun Ray 4 Policy)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

STIG ID: SUN0100
Severity: Category II
Long Name: The IAO/SA is not receiving Sun Ray security and patch notifications.
Vulnerability Discussion: Organizations need to stay current with all applicable Sun Ray Server software updates that are released from Sun. In order to be aware of updates as they are released, Sun Ray system administrators will subscribe to Sun Ray Server vendor security notices, updates, and patches to ensure that all new vulnerabilities are known. New Sun Ray Server patches and updates should be reviewed for the Sun Ray Server before moving them into a production environment.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: SUN0100 (Manual)

Ask the IAO/SA to provide actual update notification or email to verify that they are on the subscription list. The email subscription for Sun is the SunSolve Patch Club Report and it is sent out weekly by Sun. If no emails or documentation can be provided, this is a finding.

Fixes: SUN0100 (Manual)

Access Sun Microsystem's website and update your profile by going to subscriptions and select

the SunSolve Patch Club Report. This will ensure you get emails on all new and updated patches through SunSolve.

Vulnerability Key: V0016411
STIG ID: SUN0150
Release Number: 3
Status: Active
Short Name: Applications published are not approved
Long Name: Applications published to users are not approved by the IAO/SA.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 09 Sep 2008

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Sun Ray 4 Policy (Target: Sun Ray 4 Policy)
Policy: All Policies
MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

STIG ID: SUN0150
Severity: Category II
Long Name: Applications published to users are not approved by the IAO/SA.
Vulnerability Discussion: Publishing applications to users via the Kiosk mode bypasses a login mode. Therefore, some applications may or may not provide security to identify and authorize users to the application. For instance, adding the xterm application provides users with access to a command-line interface from a Kiosk mode session. This is not ideal since users should not be able to access the server's command line functionality. Therefore, only approved applications will be published to users.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: SUN0150 (Manual)
Request a copy of the documentation that lists all approved applications. If unapproved applications are published to users that are not on the list, this is a finding. If no list exists, this is a finding.
Fixes: SUN0150 (Manual)
Document and approve all published applications running on the Sun Ray network.

Vulnerability Key: V0016412
STIG ID: SUN0220

Release Number: 2
Status: Active
Short Name: Sun Ray Session Server used in hosting other apps
Long Name: The Sun Ray Session Server (SRSS) is used to host other applications.
IA Controls: DCBP-1 Best Security Practices
Categories: 12.4 CM Process
Effective Date: 09 Sep 2008

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Sun Ray 4 Policy (Target: Sun Ray 4 Policy)
Policy: All Policies
MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

STIG ID: SUN0220
Severity: Category II
Long Name: The Sun Ray Session Server (SRSS) is used to host other applications.
Vulnerability Discussion: The availability of the Sun Ray Session Server (SRSS) is critical since it manages the sessions associated with the Desktop Units. The Sun Ray software controls user authentication, encryption between Sun Ray servers and Desktop Units, system administration tools, session management, policy enforcement, and device management. If other applications are competing or using hardware resources, the availability of the SRSS may be a risk. Furthermore, application programs such as web servers, databases, or messaging systems may provide an avenue by which a privileged user may unintentionally introduce malicious code.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: SUN0220 (Manual)

Ask the IAO/SA what applications are running on the SRSS. Besides the documented UNIX services, the SRSS may have the following running as part of the Sun Ray solution and these are not applicable to this check:
- DHCP Server
- Sun Ray Connector for Windows OS

Fixes: SUN0220 (Manual)

Remove all applications that are not required for the SRSS.

Vulnerability Key: V0016413
STIG ID: SUN0240
Release Number: 2
Status: Active
Short Name: Sun Ray logs not reviewed weekly
Long Name: The Sun Ray system and user logs are not reviewed weekly.

IA Controls: ECAT-1 Audit Trail, Monitoring, Analysis and Reporting
ECAT-2 Audit Trail, Monitoring, Analysis and Reporting

Categories: 10.3 Review

Effective Date: 09 Sep 2008

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Sun Ray 4 Policy (Target: Sun Ray 4 Policy)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

STIG ID: SUN0240

Severity: Category II

Long Name: The Sun Ray system and user logs are not reviewed weekly.

Vulnerability Discussion: If a system administrator does not review Sun Ray logs weekly, there is the potential that an attack or other security issue can go unnoticed for a week or more, which is unacceptable in DoD environments.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

SUN0240 (Manual)

Critical Sun Ray log files are the administration, authentication, automatic mounting, mass storage devices, messages, and web administration. These logs are listed below. Ask the IAO/SA if Sun Ray logs are reviewed weekly.

ls-lL /var/opt/SUNWut/log | less

admin_log
auth_log
utmountd.log
utstoraged.log
messages
utwebadmin.log

If these logs are being written to an external syslog server, ask the IAO/SA if these are reviewed weekly.

Fixes:

SUN0240 (Manual)

Review Sun Ray logs at a minimum weekly.

Vulnerability Key: V0016414

STIG ID: SUN0280

Release Number: 3

Status: Active

Short Name: DRP does not include Sun Ray system

Long Name: The disaster recovery plan does not include the Sun Ray system (network infrastructure and peripherals).

IA Controls: CODP-1 Disaster and Recovery Planning
CODP-2 Disaster and Recovery Planning
CODP-3 Disaster and Recovery Planning

Categories: 13.3 Coop Plans

Effective Date: 09 Sep 2008

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Sun Ray 4 Policy (Target: Sun Ray 4 Policy)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

STIG ID: SUN0280

Severity: Category II

Long Name: The disaster recovery plan does not include the Sun Ray system (network infrastructure and peripherals).

Vulnerability Discussion: If the disaster recovery plan does not include the Sun Ray system, recovering from a disaster would not be possible. All peripherals and necessary equipment must be included in the disaster recovery plan to ensure a successful restoration of data, servers, and clients are possible.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

SUN0280 (Manual)

Ask for a copy of the site's Continuity of Operations Planning (COOP). Verify the Sun Ray system is specifically mentioned in the plan. Ensure the plan addresses the restoration of the Sun Ray system within 24 hours of activation of the COOP. Additionally, ensure that the Sun Ray system restoration is validated at least annually as part of the normal COOP testing process. If any of these requirements is not met, this is a finding.

Fixes:

SUN0280 (Manual)

Add the Sun Ray system to the COOP.

Vulnerability Key: V0016415

STIG ID: SUN0290

Release Number: 2

Status: Active

Short Name: There are no backup and recovery procedures

Long Name: There are no backup and recovery procedures for the Sun Ray system.

IA Controls: DCSD-1 IA Documentation

Categories: 13.4 Backup & Recovery

Effective Date: 09 Sep 2008

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Sun Ray 4 Policy (Target: Sun Ray 4 Policy)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

STIG ID: SUN0290

Severity: Category III

Long Name: There are no backup and recovery procedures for the Sun Ray system.

Vulnerability Discussion: Backup and recovery procedures are critical to the availability and protection of the Sun Ray system. Availability of the system will be hindered if the system is compromised, shutdown, or not available. Backup and recovery of the Sun Ray system includes the operating system, applications, and databases. Due to the complexity of the Sun Ray system and potential third party applications, procedures will need to be developed to provide guidance to system administrators. Without a process in place describing the steps to backup and recover the Sun Ray system, backups and recoveries may be inconsistent based on the system administrator performing the action. Furthermore, if a system administrator would leave the position, there will be no documentation on the process to backup or recover the system.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

SUN0290 (Manual)

Request a copy of the procedures to backup the Sun Ray system. If the documentation cannot be produced, this is a finding.

Fixes:

SUN0290 (Manual)

Produce backup documentation for the Sun Ray system.

Vulnerability Key: V0016416

STIG ID: SUN0300

Release Number: 2

Status: Active

Short Name: There is no spare Sun Ray Desktop Unit

Long Name: There is no spare Sun Ray Desktop Unit available for use in the event of a Sun Ray Desktop Unit malfunction or failure.

IA Controls: DCHW-1 HW Baseline

Categories: 13.4 Backup & Recovery

Effective Date: 09 Sep 2008

☐ Open ☐ Not a Finding ☐ Not Applicable	Comments:

☐ Not Reviewed	

Condition: Sun Ray 4 Policy (Target: Sun Ray 4 Policy)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

STIG ID: SUN0300

Severity: Category II

Long Name: There is no spare Sun Ray Desktop Unit available for use in the event of a Sun Ray Desktop Unit malfunction or failure.

Vulnerability Discussion: Users will not be able to access the required applications for their job function if the Sun Ray Desktop Unit fails or malfunctions. Having a spare Sun Ray Desktop Unit will provide users a quick replacement of the failed unit, while giving them minimal downtime.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: SUN0300 (Manual)

Ask the IOA/SA to show you where the spare Desktop Units are located in case of a failure. If no spares exist, this is a finding.

Fixes: SUN0300 (Manual)

Purchase a spare Desktop Unit in case of a failure.

Vulnerability Key: V0016417

STIG ID: SUN0350

Release Number: 2

Status: Active

Short Name: Sun Ray system not in control of site CCB

Long Name: The Sun Ray system is not under direct control of a site Configuration Control Board.

IA Controls: DCCB-1 Control Board

Categories: 10.3 Review
12.4 CM Process

Effective Date: 09 Sep 2008

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Sun Ray 4 Policy (Target: Sun Ray 4 Policy)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑

Sensitive	☑	☑	☑
Public	☑	☑	☑

STIG ID: SUN0350
Severity: Category II
Long Name: The Sun Ray system is not under direct control of a site Configuration Control Board.
Vulnerability Discussion: Security integrity of the system and the ability to back-up and recover from failures cannot be maintained without the control of the system configuration. Unless the configuration is controlled by an independent board it is much less likely to be in its approved accredited state.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks:
SUN0350 (Manual)
Ask to see the documented configuration management process for Sun Ray system.
Ensure that the plan includes a site Configuration Control Board (CCB). If a plan that includes a CCB exists, this is not a finding. If a plan exists but does not include a CCB or there is not a plan, this is a finding.
Fixes:
SUN0350 (Manual)
Implement a configuration management process for the Sun Ray system.

Vulnerability Key: V0016418
STIG ID: SUN0360
Release Number: 3
Status: Active
Short Name: Sun Ray server not configured in PNP database
Long Name: The site has not configured the Sun Ray server in the PNP database.
IA Controls: DCPP-1 Ports, Protocols, and Services
Categories: 12.4 CM Process
Effective Date: 09 Sep 2008

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Sun Ray 4 Policy (Target: Sun Ray 4 Policy)
Policy: All Policies
MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

STIG ID: SUN0360
Severity: Category II
Long Name: The site has not configured the Sun Ray server in the PNP database.
Vulnerability Discussion: DoDI 8550.1 Ports, Protocols, and Services Management (PPSM) is the DoD's policy on IP Ports, Protocols, and Services (PPS). It controls the PPS that are permitted or approved to cross DoD network boundaries. Standard well known and registered IP ports and associated protocols and

services are assessed for vulnerabilities and threats to the entire Global Information Grid (GIG) which includes the DISN backbone networks. The results are published in a Vulnerability Assessment (VA) report. Each port and protocol is given a rating of green, yellow, orange, or red in association with each of the 16 defined boundary types. Green means the protocol is relatively secure and is approved to cross the associated boundary without restrictions. Yellow means the protocol has security issues that must be mitigated to be used. Red means that the protocol is prohibited due to vulnerabilities that cannot be mitigated or approved, and is banned when crossing that boundary. The orange category requires DSAWG approval if the protocol exists and is necessary on the network. However, the orange category mandates that new systems and applications must not be developed using this protocol whether it crosses a boundary or not. The PPS Assurance Categories Assignment List (CAL) contains information regarding the assessed ports and protocols and defined boundaries, which is updated on a monthly basis. The PPSM information is available on the IASE and DKO/DoD IA Portal web sites. A portion of the DoDI 8550.1 PPS policy requires registration of those PPS that cross any of the boundaries defined by the policy that are “visible to DoD-managed components”. Therefore, to comply with the policy and ensure that protocols and ports are acceptable, Sun Ray servers will be registered as automated information systems (AIS) with their associated TCP or UDP ports in the DoD Ports and Protocol Registration System.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: SUN0360 (Manual)

If either inbound or outbound traffic to the Sun Ray server is leaving the local enclave, verify that the server has been registered in the Ports and Protocols (PNP) database (https://pnp.cert.smil.mil) for the site. If it not registered this is a finding. If the traffic is completely contained within the local enclave, this requirement does not apply.

Fixes: SUN0360 (Manual)

Register all Sun Ray traffic that is leaving the local enclave in the PNP database for the site.

Vulnerability Count - 11