IT Security Procedural Guide: Firewall and Proxy Change Request Process
CIO-IT Security-06-31

Revision 9

December 22, 2020

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 1 – June 25, 2007		
1	Bo Berlas	Updated FW change request process.	Align with new IT Service Desk process.	Throughout
2	Bo Berlas	Updated IT security policy reference.	GSA Order CIO P 2100.1D was published on 06/21/2007	4
3	Bo Berlas	Updated FW change request form in Appendix A.	Change in process flow.	9
		Revision 2 – September 27, 2007		
1	Bo Berlas	Updated step 8 – destination email address for processing of firewall change requests.	Requested by GSA Firewall Team.	6
		Revision 3 – May 02, 2008		
1	Bo Berlas	Updated steps 3 and 8 in the firewall change request process to account for usage of CA Unicenter for ticket routing.	Processing tickets directly in CA Unicenter	5-6
2	Roy Iversen	Updated FW change request form in Appendix A	Change in required data. Clarification of process.	9
		Revision 4 – June 16, 2010		
1	Iversen	Updated “Firewall Change Process”. Emphasized that the request must be at least business 5 days prior to requested change. Changed web application scan from “OWASP Top 10” to “Standard” profile. Removed requirement to remediate all Medium Risk OS vulnerabilities, changed it to recommended. Specified that ISSMs can also submit FW requests. Clarification of verification or corrected vulnerabilities.	Clarifications and ease of process.	7
2	Iversen	Renamed “Emergency” requests to “Urgent” requests.	Name change	
3	Iversen	Clarified encryption requirements. Added “Scan Requirements” section. Included use of Core Impact for OS scanning. Changed web application scan from “OWASP Top 10” to “Standard” profile. Removed requirement to remediate all Medium Risk OS vulnerabilities, changed it to recommended.	Clarifications and ease of process.	
4	Iversen	Changed firewall form.	New form simplifies process	Appendix A
5	Iversen	Updated GSA Order Reference	New revision	6

6	Iversen	Updated cover	New cover sheet	1
		Revision 5 – February 19, 2015		
1	Eriksen	Updated cover	New date and version	1
2	Eriksen	Updated Firewall Change Request process and add image showing Service Catalog	Change in process	6
3	Eriksen	All changes to the firewall access rules are processed as follows:	Change in process	6
4	Eriksen	Remove tool name from process	Removed reference to specific vulnerability scanning tool	7
5	Eriksen	Removed tool name from Operating System Vulnerability Scanning	Removed reference to specific vulnerability scanning tool	11
		Revision 6 – January 5, 2016		
1	Eriksen	Added image and information required to fill in the form	Added 2.0 Firewall Change Form	7 and 8
2	Eriksen	Removed quote from GSA Order CIO P 2100.1	Removed reference to avoid wrong information	6
3	Eriksen	Replaced Security Operations with Security Operations	Shorten the name	9-12
		Revision 7 – June 8, 2016		
1	Eriksen	Add language for Desktop firewalls	To cover Desktop Firewalls	7
2	Cozart-Amos/ Klemens	Converted to latest format and style	Conversion to latest format and style	All
		Revision 8 – June 6, 2018		
1	Feliksa/Eriksen	Updated format, structure, and style.	Biennial update.	Throughout
		Revision 9 - December 22, 2020		
1	Eriksen/ Quintananieves	Primary updates consisted of: • Clarified steps on requesting firewall changes • Added cybersecurity directives requirements • Established the proxy change request process/changed name of guide to include this process • Added a section on restricting privileged users to trusted sites	Biennial update.	Throughout

Approval

IT Security Procedural Guide: Firewall and Proxy Change Request Process, CIO-IT Security-06-31, Revision 9, is hereby approved for distribution.

X DocuSigned by: Bo Berlas FD71792616154...

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Security Operations Division (ISO) at secops@gsa.gov.

Table of Contents

List of Figures

Notes:

- Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section). Hyperlinks will be provided for external sources unless the hyperlink is to a webpage or document listed in Section 1.4. For example, Google Forms, Google Docs, and websites will have links.
- It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

1 Introduction

The General Services Administration (GSA) enterprise firewalls are an integral facet of GSA's "defense-in-depth" strategy in securing agency information and systems. It centrally controls access to systems and devices across GSA. It is imperative that strict guidelines be established and followed to ensure that only necessary and effective rules are applied to the firewall rule-base. The following sections detail the required process for all changes to the GSA firewall rule-base.

1.1 Purpose

This guide documents the firewall change request process at GSA. The guide describes the steps in the process including request initiation, vulnerability and application security scanning, and approvals.

1.2 Scope

The GSA firewall change request procedures apply to all individuals who request changes to a firewall rule-base.

1.3 Policy

GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy,"* contains the following policy statements regarding firewall change requests.

Chapter 4 Paragraph 1, Identity management, authentication and access control.

uu. OCISO must approve all requests for access through the GSA Firewall. Firewall change requests must follow the process outlined in GSA CIO-IT Security-06- 31: Firewall Change Request. This includes changes to desktop firewall and intrusion prevention systems.

vv. OCISO will block access to all external sites deemed to be a security risk to GSA. Exceptions to this policy must be approved by the CISO.

1.4 References

Federal Laws, Standards, and Publications:

- Federal Information Processing Standard (FIPS) Publication (PUB) 140-2, "*Security Requirements for Cryptographic Modules"*[1]
- FIPS PUB 140-3, "*Security Requirements for Cryptographic Modules"*

[1] Please note that while FIPS 140-3 has been released, implementation and validation is still in process and FIPS 140-2 certificates will continue to be issued.

- Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Directives

GSA Policies, Procedures, and Guidance:

- GSA CIO Order 2100.1, "*GSA Information Technology (IT) Security Policy"*

The documents below are available on the GSA IT Security Procedural Guides InSite page.

- CIO-IT Security-09-43, "*Key Management*"
- CIO-IT Security-14-69, "*SSL/TLS Implementation*"
- CIO-IT Security-17-80, "*Vulnerability Management Process*"

2 Firewall Change Request Process

The Firewall Change Request Form is available via the GSA IT Service Desk. This form is designed to assist in collecting the necessary information for the GSA IT Security Operations (SecOps) team to evaluate, approve, and implement firewall change requests. Users with an active gsa.gov account and a 'business-need' may request firewall changes. Additionally, the following minimum requirements must be met:

- All updates, development and configuration for the components involved (hardware/servers/sites/etc.) must be complete and a code freeze enforced.
- All components involved must be available and ready for evaluation.

The information required to access the Firewall Change Request Form is described below and highlighted in Figure 2-1 through 2-3, and correlated to the numbered list. Follow the steps below to access the Firewall Change Request Form:

1. Go to the GSA IT Self Service Portal
2. Select Self-Service Catalog

Figure 2-1: Self-Service Catalog

3. Select Enterprise Services

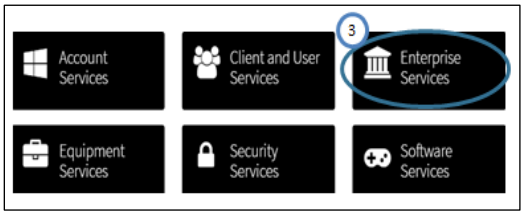

Figure 2-2: Enterprise Services

4. Select Firewall Change

Figure 2-3: Firewall Change

The following two sections describe how to complete Firewall Change Request Forms for desktop firewalls and network firewalls.

2.1 Desktop Firewall Changes

Changes to a user's Windows Firewall must be coordinated through the GSA OCISO, Security Engineering Division (ISE). The information required to complete the request is described below and highlighted in Figure 2-4, Desktop Firewall Request, and correlated to the numbered list in the figure and steps below.

Follow the steps below to complete the Firewall Change Request Form for desktop firewall changes:

1. The "Requested For" and "Opened By," fields will automatically populate the name of the Requestor.

Note: All of the fields in the "Firewall Request Information" section are required.

2. Within the "Request Type" field, select "Internal Firewall."
3. Within the "Source IP/VLAN/Network (Source is the IP Address initiating the connection)" field enter "127.0.0.1" as the IP address.
4. Within the "Business Justification for Request" field, enter a business justification explaining why the change is required.
5. Add the following note within the "Additional Comments" section: "This request pertains to a desktop firewall. Route the ticket to the SecEng Queue."

When complete, select "Add to Cart" at the bottom of the webpage to complete the order.

Once the Service Desk ticket has been created and submitted, send an email to seceng@gsa.gov, including the ticket number. Requests will normally be reviewed within five business days.

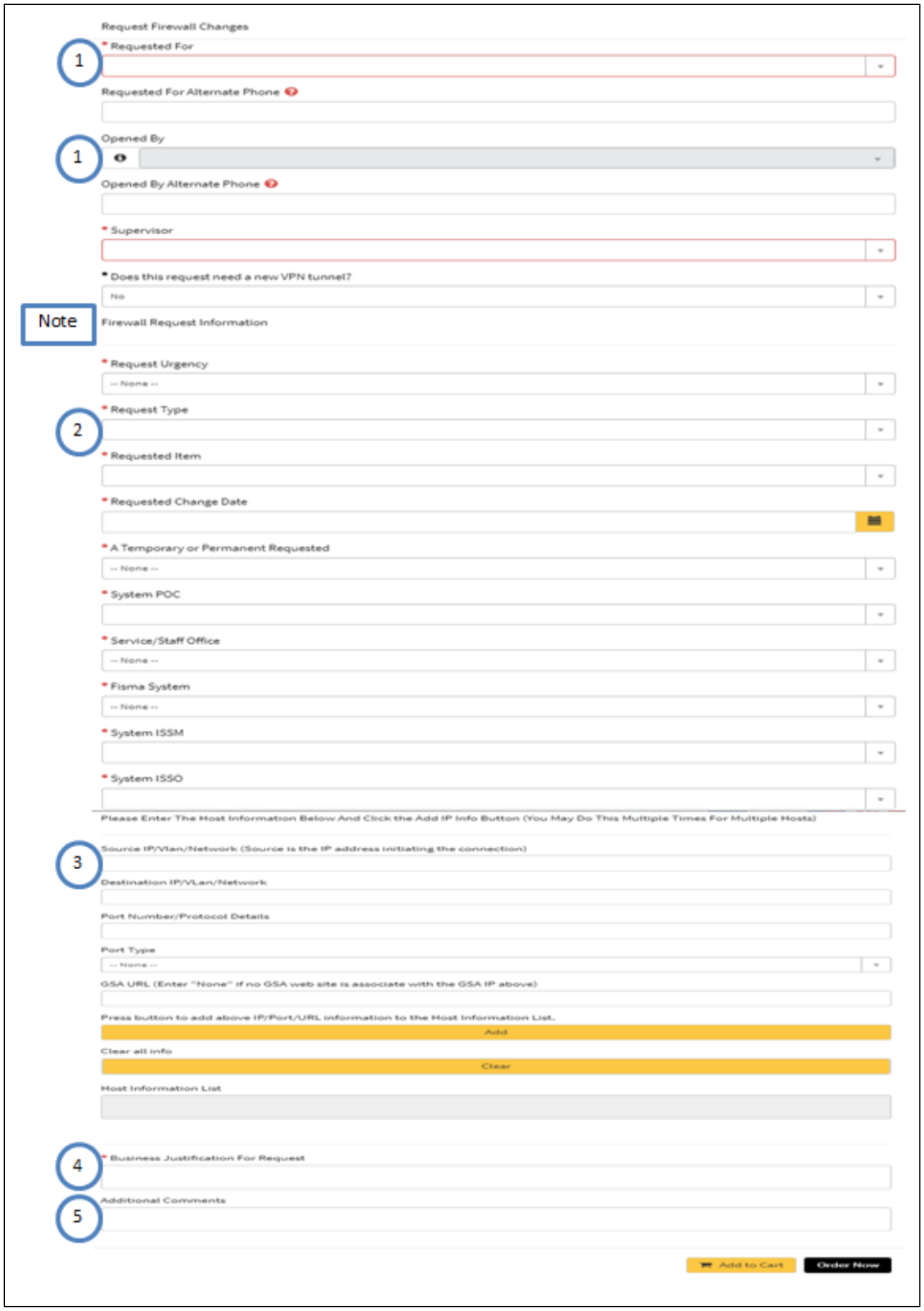

Figure 2-4: Desktop Firewall Request

2.2 Network Firewall Changes

When a change is required to GSA's external (perimeter) or internal firewall(s), a Service Catalog Request is required. For external requests, the Information System Security Officer (ISSO) or Information System Security Manager (ISSM) must submit the request **at least 5 business days ahead of the required change date.** See Section 3, for details.

The information required to complete the request is described below and highlighted in Figure 2-5, Network Firewall Request, and correlated to the numbered list in the figure and steps below.

Follow the steps below to complete the Firewall Change Request Form for network firewall changes:

1. The "Requested For" and "Opened By" fields will automatically populate the name of the Requestor.

   Note: All of the fields in the "Firewall Request Information" section are required.

2. Identify if this is a temporary or permanent change request, if temporary please put the date no longer required under "Additional Comments."
3. In the "Please Enter The Host Information Below And Click the Add IP Info Button (You May Do This Multiple Times For Multiple Hosts)" section, all fields must be completed.
4. Select the "Press button to add above IP/Port/URL information to the Host Information List." and repeat if more than one rule is needed.
5. Within the "Business Justification For Request" field, enter a business justification explaining why the change is required.

When complete, select "Add to Cart" at the bottom of the webpage and complete the order.

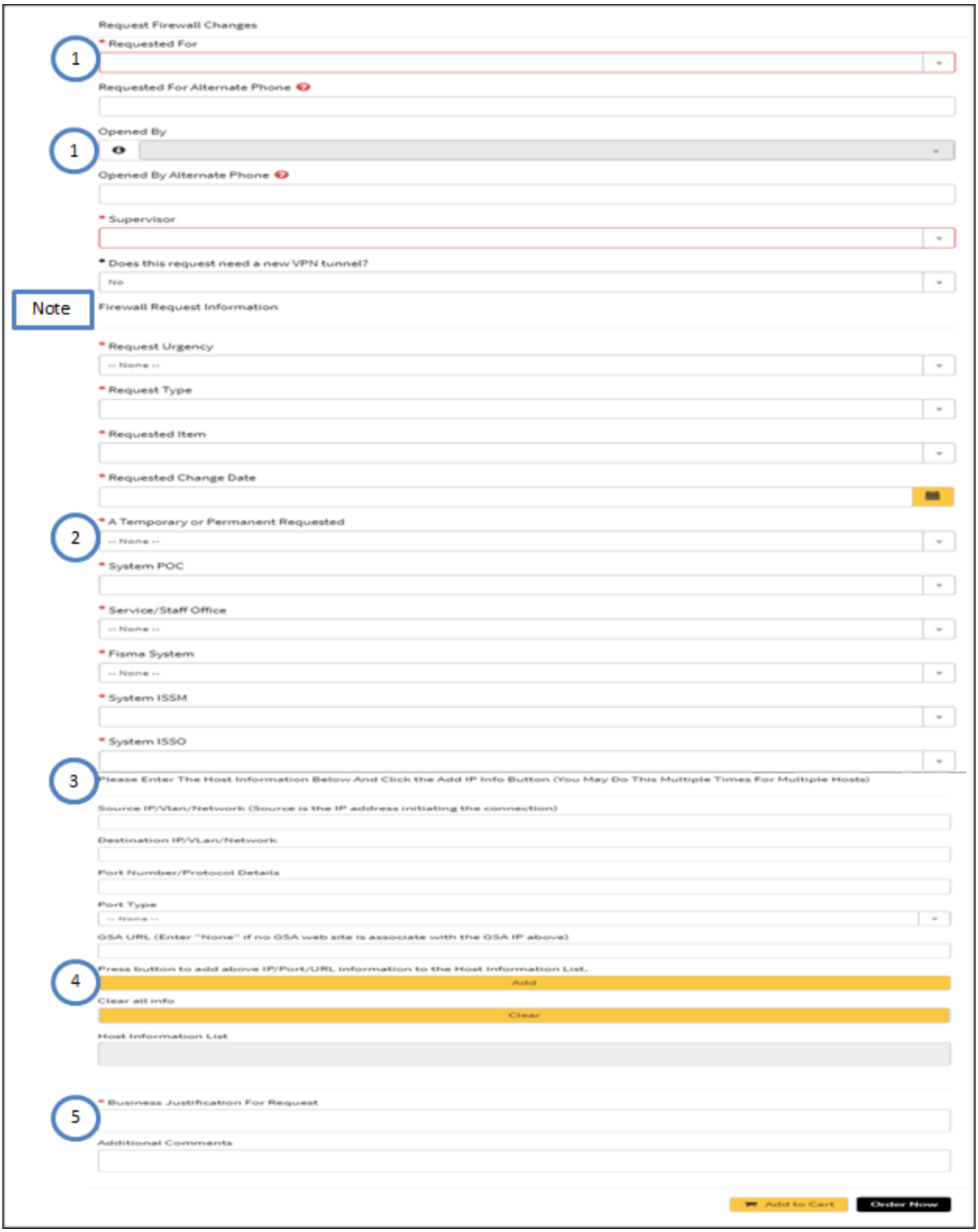

Figure 2-5: Network Firewall Request

All changes to the firewall access rules are processed as follows:

1. Individuals requiring a change to a firewall rule-base must submit a request via Service Catalog as described in Section 2. The system ISSO or ISSM must approve the change request.
2. After the ISSM or ISSO approves the request, it will be routed to **CISO.Firewall** queue.
3. Depending on the request and upon receipt of applicable logon credentials, SecOps will conduct required vulnerability scanning on all perimeter firewall change requests and web application scanning using GSA's current scanning tool(s) with the "Standard" profile, on Hypertext Transfer Protocol (HTTP) and/or Hypertext Transfer Protocol Secure (HTTPS) access requests.
4. Any required system scanning will be available within the applicable vulnerability and compliance scanning tool used by SecOps; SecOps will forward the results of the scanning activities to the ISSO for remediation and cc: the ISSM. The system should be free of High and Critical risk vulnerabilities prior to SecOps approval. See Section 4 for details.
5. Upon correction of the identified operating system (OS) and application vulnerabilities, SecOps will verify the corrective action, either manually or by rescanning.
6. Upon successful mitigation of identified vulnerabilities and ISSM approval, SecOps will assign the IT Service Desk Ticket to the **CISO.Firewall** queue with approval to process the request or deny the request.
7. Upon receipt of the approved firewall change request from SecOps , the Firewall Team will make the requested change at the appropriate time and mark the IT Service Desk Ticket – "Resolved."
8. SecOps will update the ticket to document the Service Catalog request details, approval, and the implemented firewall change.

Note: Steps 1-8 only apply to external firewall requests. Internal firewall requests typically only include steps 1, 2, 7, and 8, (e.g., Creation of the request -> Approval by ISSO or ISSM -> Firewall Team makes the change -> Ticket update).

2.3 Proxy Change Request

GSA has internal proxy servers that may require special firewall requests to allow access to internal/external resources. The information required to complete the Proxy Change Request is described below and highlighted in Figure 2-1, 2-2, and 2-4.

Follow the steps and figure below to submit a proxy change request.

1. Go to the GSA IT Self Service Portal
2. Select Self-Service Catalog (as seen in Figure 2-1)
3. Select Enterprise Services (as seen in Figure 2-2)
4. Select GSA Proxy Request

Figure 2-6: GSA Proxy Request

2.4 Restricting Privileged Users to Trusted Sites

To approve a new domain for privileged users to access a trusted site, employees and contractors with privileged accounts (i.e., Short Name Accounts [SNAs]) must submit a GSA Proxy Request through the GSA Self-Service Catalog. This process will apply if privileged users are working with a vendor or new application that requires access to a specific domain from an SNA account and the domain has not already been approved, and will require approval by the ISSO/ISSM and the Director of Security Operations or CISO. Before submitting this request, refer to the full list of approved domains. If the requested site is already approved, then a new Service Catalog request is not required.

Follow the steps below to request to approve a new site:

1. Go to the GSA IT Self Service Portal
2. Select Self-Service Catalog (as seen in Figure 2-1)
3. Select Enterprise Services (as seen in Figure 2-2)
4. Select GSA Proxy Request (as seen in Figure 2-6)

3 Prioritization of Firewall Change Requests

Two priority categories can be submitted for firewall changes; normal and priority.

3.1 Normal Change Requests

Normal or routine firewall change requests require at least 5 business days advance notice prior to the requested change date. During this period, SecOps will conduct required OS and application testing, with retesting following vulnerability mitigation (if any). SecOps will coordinate any necessary approvals

Firewall change requests may exceed 5 business days if coordination with the ISSM, ISSO, and/or applicable system points of contact (POCs) becomes an issue and/or it takes a long time to mitigate vulnerabilities.

3.2 Urgent (Emergency) Change Requests

In urgent situations, firewall change requests supporting key business functions may be communicated verbally with the Security Operations (ISO) Director. These requests must be

preapproved by the System Owner, Program Manager, or ISSM and followed up with appropriate documentation. SecOps will put forth a best effort to facilitate the completion of urgent change requests. Such requests must undergo OS and application security testing and have High and Critical Risk vulnerabilities mitigated.

4 Reviewing the Firewall Change Request

4.1 Technical Review of Firewall Request

Upon receipt of the completed Firewall Change Request Form, SecOps will review the request to assure that only the required minimum access is requested and that insecure ports and/or services are not opened to the Internet.

As a rule, services such as file transfer protocol (FTP), Telnet, and other protocols that send sensitive data (e.g., log-in/authentication data) in the clear are generally not approved for perimeter changes.

Encryption must use FIPS 140-2[2] certified encryption modules, this implies transport layer security (TLS), as secure sockets layer (SSL) encryption is not FIPS certified. For more information, download the following GSA IT procedural guides from the IT Security Procedural Guides InSite page:

- CIO-IT Security-09-43, "*Key Management*"
- CIO-IT Security-14-69, "*SSL/TLS Implementation*"

4.2 System Scan Requirements

OS vulnerability scans are normally required for all perimeter requests, and web application scanning for any request for HTTP or HTTPS protocols.

4.2.1 Operating System Vulnerability Scanning

OS vulnerability scans will be conducted with authentication where applicable. The credentials used typically require administrator level privileges to run successful scans.

SecOps has preconfigured credentials that should be used for this - contact the SecOps scan team for the details.

The following conditions should be satisfied prior to SecOps approval:

1. The system is included in a Federal Information Security Modernization Act (FISMA) inventory as listed in the GSA Enterprise Architecture Analytics and Reporting (GEAR)

[2] Ibid., 1.

FISMA inventory and scanned as part of the enterprise vulnerability management program (see CIO-IT Security-17-80, "*Vulnerability Management Process*"), AND
2. There are no outstanding Critical risk vulnerabilities with Common Vulnerability Scoring System (CVSS) base score 9.0; AND
3. There are no active High risk vulnerabilities with CVSS base score 7.0 older than 14 days.

Each request is evaluated individually, and approval is at the discretion of the SecOps team.

4.2.2 Web Application Scanning

If applicable, change requests involving HTTP and/or HTTPS access will be scanned using GSA's vulnerability scanning tool.

4.2.3 Cybersecurity Directives Compliance Scanning

All Firewall requests that will open a system to the public Internet must be scanned for compliance with all DHS CISA Directives.

4.3 Exceptions to Scanning

Scanning may be waived at the discretion of the CISO or Director of SecOps or their delegated staff. Typically, one of the following two criteria must be satisfied in order for scanning to be waived:

1. Criteria #1
    a. The request is to change or add a single Internet IP or a limited Internet IP range to an existing firewall rule, AND
    b. The system is included in GSA's FISMA inventory and scanned as part of the enterprise vulnerability management program AND
    c. There are no Critical risk vulnerabilities (i.e., CVSS base score 9.0 or above), AND
    d. There are no High risk vulnerabilities (i.e., CVSS base score 7.0 or above) older than 14 days

OR

2. Criteria #2
    The request is to make a minor change to an existing firewall rule that was put in place within the last 45 days and the system does not have any known outstanding vulnerabilities.