



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

**Revision 8**

June 6, 2018

## VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason For Change	Page Number of Change
<b>Revision 1 – June 25, 2007</b>				
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
<b>Revision 2 – September 27, 2007</b>				
1	Bo Berlas	Updated step 8 - destination email address for processing of firewall change requests.	Requested by GSA Firewall Team.	6
<b>Revision 3 – May 02, 2008</b>				
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
<b>Revision 4 – June 16, 2010</b>				
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
<b>Revision 5 – February 19, 2015</b>				
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
<b>Revision 6 – January 5, 2016</b>				
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
<b>Revision 7 – June 8, 2016</b>				
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
<b>Revision 8 – June 6, 2018</b>				
1	Feliksa/ Eriksen	Updated format, structure, and style.	Biennial update.	Throughout

## Approval

IT Security Procedural Guide: Firewall Change Request Process, CIO-IT Security 06-31, Revision 8 is hereby approved for distribution.

6/14/2018

**X** Kurt Garbars

---

Kurt Garbars  
GSA Chief Information Security Officer  
Signed by: KURT GARBARS

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

## Table of Contents

<b>1</b>	<b>Introduction</b> .....	<b>1</b>
1.1	Purpose .....	1
1.2	Scope.....	1
1.3	Policy .....	1
1.4	References .....	1
<b>2</b>	<b>Firewall Change Request Process</b> .....	<b>2</b>
2.1	Desktop Firewall Changes .....	3
2.2	Network Firewall Changes .....	5
<b>3</b>	<b>Prioritization of Firewall Change Requests</b> .....	<b>7</b>
3.1	Normal Change Requests.....	7
3.2	Urgent (Emergency) Change Requests .....	8
<b>4</b>	<b>Reviewing the Firewall Change Request</b> .....	<b>8</b>
4.1	Technical Review of Firewall Request.....	8
4.2	System Scan Requirements.....	8
4.2.1	Operating System Vulnerability Scanning.....	8
4.2.2	Web Application Scanning .....	9
4.3	Exceptions to Scanning .....	9

## List of Figures

<b>Figure 2-1</b>	<b>– Selecting the Firewall Change Form</b> .....	<b>2</b>
<b>Figure 2-2</b>	<b>– Desktop Firewall Request</b> .....	<b>4</b>
<b>Figure 2-3</b>	<b>– Network Firewall Change Request</b> .....	<b>6</b>

## 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" states:

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

- [FIPS PUB 140-2](#), "Security Requirements for Cryptographic Modules"

#### **GSA Guidance:**

- [GSA Order CIO 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"

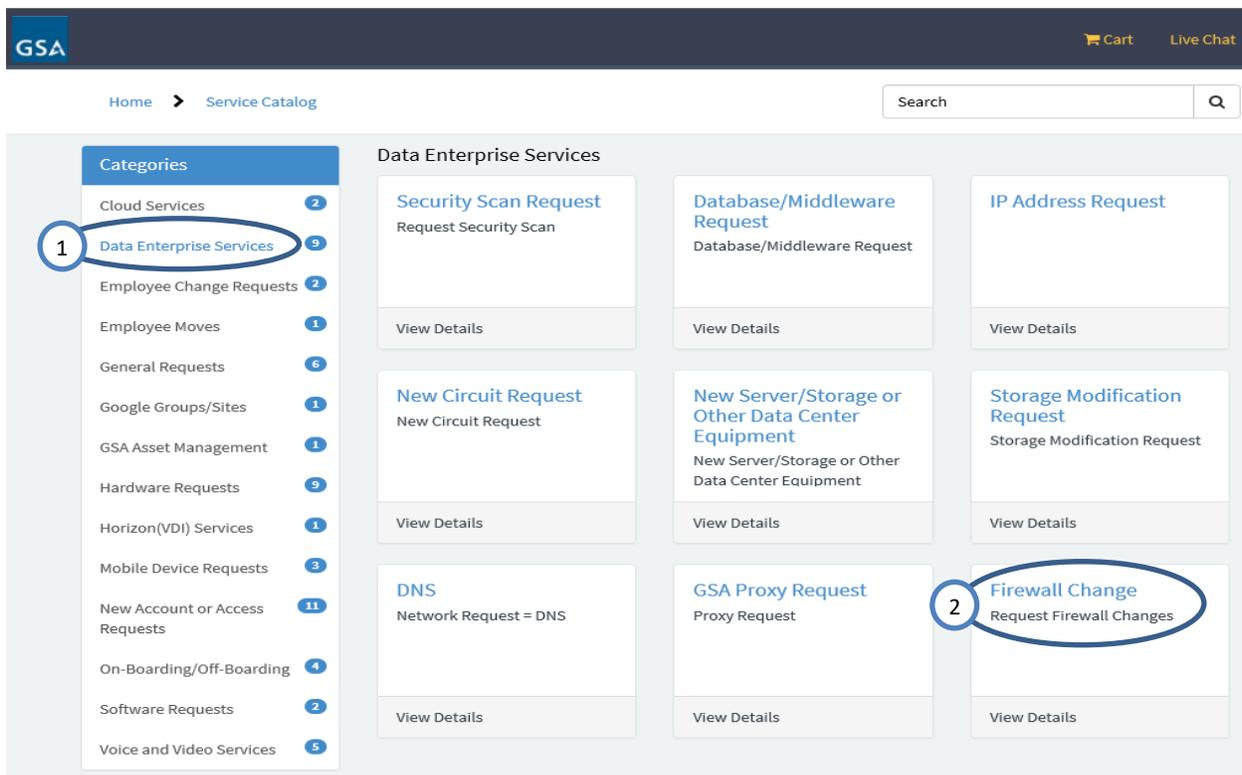
## 2 Firewall Change Request Process

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.

Users may request a firewall change by opening the [GSA InSite](#) home page and clicking on “Submit a Service Ticket” in the IT Service section. Upon opening the GSA Service-Now support page, select the option “Order Something.” Once Figure 2-1 is displayed, follow steps 1 and 2 below to access the “Firewall Change” form.

1. Select Data Enterprise Services
2. Select Firewall Change



**Figure 2-1 – Selecting the Firewall Change Form**

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 Office of the Chief Information Security Officer (OCISO), Security Engineering Division (ISE). The information required to complete the request is described below and highlighted in Figure 2-2, Desktop Firewall Request, and correlated to the numbered list.

Follow the steps below to complete the Firewall Change Form:

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

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

2. Select "Internal Firewall" as the Request Type.
3. Within Source IP/VLAN/Network 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 [ise-guides@gsa.gov](mailto:ise-guides@gsa.gov) including the ticket number. Requests will be reviewed within five business days.

The image shows a web-based form titled "Requesters Information" and "Firewall Request Information".

- 1**: Callout pointing to the "Requested For" dropdown menu.
- 1**: Callout pointing to the "Opened By" dropdown menu.
- Note**: A blue-bordered box containing the word "Note" is positioned above the "Request Type" dropdown.
- 2**: Callout pointing to the "Request Type" dropdown menu.
- 3**: Callout pointing to the "Source IP/Vlan/Network" input field.
- 4**: Callout pointing to the "Business Justification For Request" text area.
- 5**: Callout pointing to the "Additional Comments" text area.

The form includes fields for "Requested For Alternate Phone", "Opened By Alternate Phone", "Supervisor", "Request Urgency", "Requested Item", "Requested Change Date", "System POC", "Service/Staff Office", "Fisma System", "System ISSM", "System ISSO", "Host Information List", and "Additional Comments". There are also "Add" and "Clear" buttons for the host information list.

Figure 2-2 – 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 2-3, Network Firewall Change Request, and correlated to the numbered list.

Follow the steps below to complete the Firewall Change Form:

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

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

2. 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.
3. Select Add IP/Port/URL info and repeat if more than one rule is needed.
4. 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.

Requesters Information

Requested For 1

Requested For Alternate Phone

To see the primary number please select the icon next to Requested For name.

Opened By 1

Opened By Alternate Phone

To see the primary number please select the icon next to Opened By name.

\* Supervisor

Firewall Request Information Note

\* Request Urgency  
-- None --

\* Request Type

\* Requested Item

\* Requested Change Date

\* System POC

\* Service/Staff Office  
-- None --

\* Fisma System  
-- None --

\* System ISSM

\* System ISSO

Please Enter The Host Information Below And Click the Add IP Info Button (You May Do This Multiple Times For Multiple Hosts) 2

Source IP/Vlan/Network (Source is the IP address initiating the connection)

Destination IP/Vlan/Network

Port Number/Protocol Details

Port Type  
-- None --

GSA URL (Enter "None" if no GSA web site is associate with the GSA IP above)

Press button to add above IP/Port/URL information to the Host Information List.

Add 3

Clear all info

Clear

Host Information List

\* Business Justification For Request 4

Additional Comments

Figure 2-3 – Network Firewall Change 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. 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 HTTP and/or 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 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 OCISO Security Operation Division (ISO) 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 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 -> FW Team makes the change -> Ticket update).

### 3 Prioritization of Firewall Change Requests

There are two priority categories that 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 and will retest following vulnerability mitigation (if any) and coordinate necessary approvals.

Firewall change requests may exceed 5 business days if coordination with the ISSM, ISSO, and/or applicable system points of contact (POC) 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. 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, 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 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 certified encryption modules, generally this implies TLS, as 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) 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 CVSS base score 10.0; 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.

#### 4.3 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 outstanding Critical risk vulnerabilities with CVSS base score 10.0, AND
- d. There are no active High risk vulnerabilities with CVSS base score 7.0 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.