

Office of Information and Technology,  
 Office of Field Security Operations,  
 Security Configuration Management Service,  
 Enterprise Security Change Control Board  
 Change Request



The VA ESCCB is established to provide a board charged with the responsibility for ensuring all proposed changes to VA are reviewed to ensure that they are viable and will not adversely impact the operation of the existing system or subsystem. The Change Request (CR) will be the primary

<b>ESCCB Change Request (Decision):</b>	<b>Date:</b>
<b>Title of ESCCB Change Request: IPv6 Testing for OMB</b>	
<b>Change Initiator/Project Manager: Craig Wasson</b>	
<b>Date: 2/6/2007</b>	
<b>Type of Submission:</b>	
New ESCCB Request.....	<input checked="" type="checkbox"/>
Modification to Existing ESCCB Request.....	<input type="checkbox"/>
Documentation Update (does not go out for ESCCB vote).....	<input type="checkbox"/>
<b>Type of Change:</b>	
New Access into/out of the VA.....	<input checked="" type="checkbox"/>
Change to Existing Access.....	<input type="checkbox"/>
Previous Request Numbers (if known)	
<b>ESCCB CR#:</b>	<b>VANSOC Ticket#:</b> <b>Gway Conn. ID#:</b>

<p>change instrument used to propose changes to VA System Configurations. All approved CRs will be scanned and archived along with any supporting documentation.</p> <p>Fill out the CR completely and submit using signed and encrypted email. Attach supporting documents to the email containing the request. Inaccurate or missing information will lead to delays in review and approval.</p> <p>For administrative support, contact Kevin Warren at (202) 756-1966 or kevin.warren@va.gov For technical support, contact the VANSOC Help Desk at 800-877-4328 or vainoc@va.gov.</p>	<p><b>Type of Request:</b></p> <p><b>External Connection (Complete Section I).....</b> <input type="checkbox"/></p> <p>    Business Partner Gateway..... <input type="checkbox"/></p> <p>    LAN Extension VPN..... <input type="checkbox"/></p> <p>    Non-VA (outbound) VPN Client..... <input type="checkbox"/></p> <p>    Site to Site VPN..... <input type="checkbox"/></p> <p><b>VA Web Server (Complete Section II).....</b> <input type="checkbox"/></p> <p>    Access to VA web servers from the internet.</p> <p><b>Remote Control Waiver (Complete Section III).....</b> <input type="checkbox"/></p> <p>    Temporary permission to allow an outside Vendor to take remote control of a VA system. This includes Web-based Remote Access Applications.</p> <p><b>Firewall Waiver (Complete Section IV).....</b> <input type="checkbox"/></p> <p>    Access to internet servers from the VA.</p> <p><b>Other (Refer to Section V).....</b> <input checked="" type="checkbox"/></p> <p>    The use of 'Other' is discouraged and should be used only for requests that cannot be described using the preceding sections.</p>
<p><b>Type of Data?</b></p> <p>    <b>1. Is data being collected on this system?</b></p> <p>        <b>a. If yes, what data types are being collected? (i.e. PII data, PHI data, etc..)</b></p> <p>        <b>b. What is the mechanism for collecting this data?</b></p> <p>        <b>c. Who has access to this data and what level of access?</b></p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>

**2. Is data being stored on this system?**

**a. If yes, what data types are being store? (i.e. PII data, PHI data, etc..)**

**b. What is the security protection controls for this data?**

**c. Who has access to this data and what level of access?**

Yes  No

## Section I: External Connection Request

### (Business Partner Gateway, LAN Extension, Non-VA VPN Client, Site to Site VPN)

Obtain a copy of any the documents referenced below from the One-VA VPN Portal at <https://vaww.admin.vpn.va.gov/one-va-vpn/home/site2site.html>. For technical assistance with any of these forms, contact the One-VA VPN Helpdesk at 1-800-877-4328.

ESCCB		Comments
1	Is this a request for a Business Partner Gateway?	Yes <input type="checkbox"/> No <input type="checkbox"/>
	Attach a completed VA 10-0437 External Connection Request. (VHA only, all others disregard this form)	
	Attach a completed BPG worksheet.	
	Is this a request for a new connection?	Yes <input type="checkbox"/> No <input type="checkbox"/>
	Attach a completed CONOPS.	
	Attach a completed OCIS C&A Division MOU/ISA Review.	
	Attach a completed MOU/ISA that is signed by the Business Partner.	
	Attach completed IPS POC and Activation documents.	
	Attach a completed POC form.	
2	Is this request for a LAN Extension to a VA facility?	Yes <input type="checkbox"/> No <input type="checkbox"/>
	Attach a completed LAN Extension worksheet.	
	Is this a request for a new connection?	Yes <input type="checkbox"/> No <input type="checkbox"/>
	Attach a completed CONOPS.	
	Attach a completed POC form.	
3	Is this a request for a VPN Client to access non-VA resources?	Yes <input type="checkbox"/> No <input type="checkbox"/>
	Attach a completed Outbound VPN MOU/ISA that is signed by the Business Partner. Note: The MOU/ISA must state that the Business Partner's VPN device does not allow VA clients to perform split tunneling.	

ESCCB		Comments
	<b>Is this a SSL or an IPsec VPN?</b>	Yes <input type="checkbox"/> No <input type="checkbox"/>
<b>4</b>	<b>Is this a request for a Site to Site VPN?</b>	Yes <input type="checkbox"/> No <input type="checkbox"/>
	<b>Attach a completed S2S worksheet.</b>	
	<b>Is this a request for a new connection?</b>	Yes <input type="checkbox"/> No <input type="checkbox"/>
	<b>Attach a completed CONOPS.</b>	
	<b>Attach a completed OCIS C&amp;A MOU/ISA Review.</b>	
	<b>Attach a completed MOU/ISA that is signed by the Business Partner.</b>	
	<b>Attach a completed POC form.</b>	
<b>5</b>	<b>Summary</b> (Describe the change.)	
<b>6</b>	<b>Justification</b> (Why is the change needed?)	
<b>7</b>	<b>Urgency</b> (What is the required timeline and impact of delays?)	
<b>8</b>	<b>Systems Impacted</b> (Where systems are impacted by the change, describe any modifications that must be made to the system in order to accommodate the change.)	
<b>9</b>	<b>Attach Project Plan</b> (Include dates and deliverables)	
<b>10</b>	<b>Attach any other Supporting Documentation</b>	
<b>11</b>	<b>Attach digitally signed approval email from appropriate authority.</b> (VISN CIO, Program Office, or Business Unit Director)	
<b>12</b>	<b>Attach any other Supporting Documentation</b>	
<b>13</b>	<b>Provide any comments which you may feel are important.</b>	

## Section II: VA Web Server Request

	ESCCB	Comments
1	VA entity making request:	VHA <input type="checkbox"/> VBA <input type="checkbox"/> CEM <input type="checkbox"/> OIG <input type="checkbox"/>  WEBOPS <input type="checkbox"/> AAC <input type="checkbox"/> OTHER:
2	Internal VA IP address of Server:	
3	Web Application Name:	
4	Web Server physical location: Note: If the web server is not hosted by VA WebOps, the server must be located in a DMZ at the facility.	
5	Requested VA Internet FQDN (Fully Qualified Domain Name) for server:	
6	Internal VA FQDN (Fully Qualified Domain Name) for server:	
7	Web Site Aliases?	
8	Type of Web Application (e.g. Oracle, OWA, SAP, ...)	
9	Type of Web Server (IIS, Apache, etc...)	
10	Must the Internet source address be presented? If so, provide the reason(s). The One-VA gateways NAT Internet source IP addresses so they normally would not be visible on server logs.	Authentication <input type="checkbox"/> Reporting <input type="checkbox"/> Other (explain):
11	Are there multiple servers? If there are multiple servers in a server farm, please answer questions 12, 13 and 14. Otherwise skip to question 15:	Yes <input type="checkbox"/> No <input type="checkbox"/>
12	Are the web servers mirrored?	Yes <input type="checkbox"/> No <input type="checkbox"/>
13	Are the web servers clustered?	Yes <input type="checkbox"/> No <input type="checkbox"/>
14	Are the web servers load balanced?	Yes <input type="checkbox"/> No <input type="checkbox"/>
15	Is this server an HTTPS server? If so, answer question 16, otherwise skip to 17	Yes <input type="checkbox"/> No <input type="checkbox"/>
16	Is TLS enabled and SSL 2 and SSL 3 disabled?	Yes <input type="checkbox"/> No <input type="checkbox"/>

17	<b>What web browsers does your website support?</b>	Only IE version 5.0 and above <input type="checkbox"/> IE, Mozilla, and Netscape <input type="checkbox"/> Any other web browser <input type="checkbox"/>
18	<b>Does your website use Java Applets, Active X controls, VBScripts or Flash which generate HTTP Requests, cookies or sticky bit?</b>	Yes <input type="checkbox"/> No <input type="checkbox"/>
19	<b>Does your website host multimedia content?</b>	Yes <input type="checkbox"/> No <input type="checkbox"/>
20	<b>Does your website host sensitive data?</b>	Yes <input type="checkbox"/> No <input type="checkbox"/>
21	<b>Attach any other Supporting Documentation</b>	
22	<b>Provide any comments which you may feel are important.</b>	

### Section III: Remote Control Waiver Request

!!! Remote Control Waivers are provided for short term emergency communication only. If Remote Control of a system is needed on an ongoing basis, an External or a One-VA VPN Client connection should be setup to carry the Remote Control communication. A Waiver will be granted for a particular system ONLY ONCE. Any future Waiver Requests for that system will be denied if an External Connection Request for that system has not been filed with ESCCB. !!!

The Remote Control session must be performed using a Windows account that has the lowest privileges needed to accomplish the required task, after which the connection must be terminated. The VA POC designated by the ISO is responsible for actively monitoring all remote control activities.

	ESCCB	Comments
1	<b>Summary</b> (Describe the change.)	
2	<b>Justification</b> (Why is the change needed?)	
3	<b>Urgency</b> (What is the required timeline and impact of delays?)	
4	<b>Systems Impacted</b> (Where systems are impacted by the change, describe any modifications that must be made to the system in order to accommodate the change.)	
5	<b>Attach Project Plan</b> (Include dates and deliverables)	
7	<b>Host Name of VA system to be accessed</b>	
8	<b>IP Address of VA system to be accessed</b>	
9	<b>URL of internet based Remote Access server (if one is used)</b>	
10	<b>Vendor who is Remotely Accessing VA equipment</b>	

<b>11</b>	<b>Duration of access</b> (Access will not be approved for more than 36 hours)	
<b>12</b>	<b>Start date/time</b>	
<b>13</b>	<b>End date/time</b>	
<b>14</b>	<b>Attach approved C&amp;A SLCA and ATO that identifies this system as a critical system:</b>	
<b>15</b>	<b>Include item in SMART POA&amp;M database:</b>	
<b>16</b>	<b>Attach Email including local CIO, ISO, RISO approval</b>	
<b>17</b>	<b>Attach digitally signed approval email from appropriate authority.</b> (VISN CIO, Program Office, or Business Unit Director)	
<b>18</b>	<b>Attach any other Supporting Documentation</b>	
<b>19</b>	<b>Provide any comments which you may feel are important</b>	

## Section IV: Firewall Waiver Request

ESCCB		COMMENTS				
1	Is this connection <u>always initiated</u> by a system inside the VA?	Yes <input type="checkbox"/>	No <input type="checkbox"/>			
2	Is sensitive data transferred? (i.e. Patient Data ,SSN etc)	Yes <input type="checkbox"/>	No <input type="checkbox"/>			
3	Describe the data transferred.					
4	What type FIPS 140-2 encryption (if any) is used?					
5	Business Justification.					
6	Attach any other Supporting Documentation					
7	Provide any comments which you may feel are important					
<b>Connection Requirements for Firewall Rules</b> for a list of TCP&UDP port numbers, refer to IETF RFC 1700						
Internal VA IP Address	Remote Internet IP Address	Port # 80=http 443=https etc.	Protocol tcp/udp/ esp/icmp/ hl7	Traffic Originated By		Comments  Identify the application utilizing the specified port and protocol
				VA	Remote	
2001:4830:1631:501::3	2001:420:2200:1::3	80	tcp		x	Internet Explorer
2001:4830:1631:501::3	2001:420:2200:1::3	21	tcp		x	FTP
2001:4830:1631:501::3	2001:420:2200:1::3	33434	udp		x	Traceroute
2001:4830:1631:501::3	2001:420:2200:1::3		icmp		x	Ping, Traceroute
2001:4830:1631:303::3	2001:420:2200:1::3	80	tcp	x		Internet Explorer
2001:4830:1631:303::3	2001:420:2200:1::3	21	tcp	x		FTP

2001:4830:1631: 303::3	2001:420:2200:1:: 3	33434	udp	x		Traceroute
2001:4830:1631: 303::3	2001:420:2200:1:: 3		icmp	x		Ping, Traceroute
2001:4830:1631: 204::3	2001:420:2200:1:: 3	80	tcp	x		Internet Explorer
2001:4830:1631: 204::3	2001:420:2200:1:: 3	21	tcp	x		FTP
2001:4830:1631: 204::3	2001:420:2200:1:: 3	33434	udp	x		Traceroute
2001:4830:1631: 204::3	2001:420:2200:1:: 3		icmp	x		Ping, Traceroute
2001:4830:1631: 403::3	2001:420:2200:1:: 3	80	tcp	x		Internet Explorer
2001:4830:1631: 403::3	2001:420:2200:1:: 3	21	tcp	x		FTP
2001:4830:1631: 403::3	2001:420:2200:1:: 3	33434	udp	x		Traceroute
2001:4830:1631: 403::3	2001:420:2200:1:: 3		icmp	x		Ping, Traceroute


## Section V: Other

If there is insufficient space on the form, you may add additional details here.

You may also use this section to describe requests that do are not adequately described in sections I-IV. In this case, all approvals and supporting documentation required by sections I-IV should be included. Note that the use of 'Other' to describe a request is discouraged. Sections I-IV **must be used** to describe a request if at all possible.

Per OMB Memorandum 05-22 the VA must deploy IPv6 over the core network and to the Internet by June 30, 2008. To accomplish this a task force was created to develop an IPv6 test and implementation plan. Attached to this request is the test plan and risk assessment which this team developed. The IPv6 team wishes to complete this task well before the June 30 deadline and has set a target of completing this testing by March, 2008.

This request has two supporting documents attached. A test plan is attached which has all of the details concerning the hardware and network addresses to be used. It also describes how we will conduct the tests to meet the OMB requirements. A risk assessment document is also attached which describes how we will identify and mitigate risks to the VA network while we perform the IPv6 test.

The OMB IPv6 mandate has 3 requirements:

### 1. INBOUND

Transmit IPv6 traffic from the Internet and external peers, through the network backbone (core), to the LAN.

### 2. OUTBOUND

Transmit IPv6 traffic from the LAN, through the network backbone (core), out to the Internet and external peers.

### 3. INTERNAL

Transmit IPv6 traffic from the LAN through the network backbone (core), to another LAN (or another node on the same LAN).

To accomplish the inbound and outbound requirement we propose to implement an IPv6 Internet connection in the Dallas ECSIP gateway. This connection will be provided by an IPv6 over IPv4 tunnel to a SixXS IPv6 POP located in Ashburn, VA. This traffic will be forwarded to the VA backbone using a Cisco PIX 515e firewall which will be dedicated to only forwarding IPv6 traffic. This firewall will parallel the existing ECSIP firewalls and will not be configured to accept or forward any IPv4 traffic.

To carry traffic over the backbone we propose using GRE tunnels between the WAN routers in the Dallas ECSIP gateway and the WAN routers at the 3 internal VA test locations. These locations are Hines, IL, Little Rock, AR and Falling Waters, WV.

At these 3 locations we propose to enable IPv6 on the local LANs to provide access to the individual end devices which will be running IPv6. The attached test plan describes in more detail how this will be implemented.

This will only be a temporary implementation. Once we have demonstrated our ability to run IPv6 to the satisfaction of the OMB we will disable IPv6 until the VA has a business requirement to permanently implement it.

To meet the security requirement of the ECSIP gateway we will limit IPv6 traffic to only the specific source and destination hosts that are documented in the test plan. All other IPv6 traffic will be blocked by the IPv6 firewall. The IPv6 traffic will be monitored by existing IPS devices within the Dallas ECSIP gateway which are already IPv6 capable. Attached is the risk assessment the IPv6 team developed to insure we were identifying potential risks and mitigating those risks to the greatest extent possible.

