External Connectivity User Guide

citi

Contents

Purpose

The purpose of this guide is to document for a requester the change submission process for several classes or types of network security changes. These classes of changes will result in some sort network level access change to some portion of the Citi network. The five types of network changes that are covered here are:

- Firewall Change Requests
- Proxy Change Requests
- Security Access Control List (SEC_ACL) Change Requests
- IP Registration Requests
- Third Party Access AppSense Request

This guide includes instructions for the following:

1) The process for submitting a change for each type of request is covered in detail using Citi Marketplace
2) Instructions on how to use the Citi Marketplace tool.
3) The prerequisites for submitting requests that are the responsibility of the business
4) The requirements and focus of the ISO review which is required for several types of requests
5) Instructions on possible sources of required technical information for requests and how to provide this information to the External Connectivity Management (ECM) team which processes all requests.
6) The process for attesting to the continued need of a change request via the Annual Connectivity Verification. This attestation is done through the Citi Connectivity Registry (CCR).

Prerequisites

The following items are prerequisites for submitting all External Connectivity Requests. The requester is required to complete these items, prior to submitting a CMP request. Failure to do so will result in processing delays.

Area	Requirements
CTI Project Request	This step is highly recommended if the requester does not have a full understanding of the technical or networking requirements, and the necessary configuration changes, to meet their needs. It is stongly suggested all project coordinators to engage a CTI engineer for assistance as a way to ensure the correct request is being made. To initiate the CTI Project download the Networks Design Document (https://catecollaboration.citigroup.net/domains/networks/processes/Pages/Networks_Project_Templates.aspx), complete all required fields on the Base Scope tab. Next, open a MarketPlace Project Request [https://cmp.nj.ssmb.com/marketplace/control/product/~productId=47306_21653_GLOBAL#] fill out the appropriate information and attach the Network Design Document to the Marketplace request. If you require additional assistance on Marketplace submission please review the CTI user guide (https://collaboration.citiemployeeservices.citigroup.net/sites/CNPS/Training/Training/CTI%20Project%20Request%20in%20Citi%20Marketplace%20and%20ResolveIT/Requestor%20-%20Overview.doc) Once the form is reviewed by Project Delivery, it will be assigned to the appropriate engineering team to begin definition and design. The network connectivity design created by CTI should be used as a reference point as you proceed through this document.
Citi Approved Supplier Program (CASP)	All requests involving a 3rd Party (Vendor, Supplier, Partner, Client, Government Agency…) will require a corresponding CASP entry. This is required for vendors and non-vendors; however, non-vendors are not subject to the vendor assessment requirement of CASP It is possible that the third party may already be regsitered in CASP even if your business did not initiate the registration. It is therefore recommended that you perform a thorough search prior to initiating a new CASP registration via the Supplier Search page (https://casp.ny.ssmb.com/casp/asp/splash.asp). For third party vendors not yet registered in CASP: The business should contact Citi Procurement Services (CPS) to initiate the process to qualify the vendor as an approved supplier in CASP (email to: ESRM CASP). This should be done during the connectivity design phase, so that it does not impact the lead time to implement the connection. For non-vendor third parties not yet registered in CASP, follow these steps to register a non-vendor third party in the CASP database: Go to the CASP web page (https://casp.ny.ssmb.com/casp/asp/casp_submenu.asp?menu=10&section_title=20&section=10). Accept the Form agreements. Under General Forms select intranet CASP Request Form (iCRF).

Area	Requirements
	Accept the agreement.
	Type the Supplier Name that needs to be added to CASPS
	Select Create ICRF at the top right hand side of the screen.
	In Section 1.1 of the form, select the option "Add/Reactivate Client or Partner for CCR Registration Only."
	In Section 1.1.2, select "Client for CCR purposes only."
	Fill out Section 2 – Supplier Information, Section 3 – Business Relationship Information and Section 4 – Contacts.
Citi Systems Inventory (CSI)	All Citi systems that will be accessed by a third party must be registered in the CSI database maintained by CTI. It is possible that the system may already be registered in CSI even if your own business did not initiate the registration. It is therefore recommended that you perform a thorough search prior to initiating a new registration via the advanced search page (https://archcntr.nam.nsroot.net/archcntr/tools/archcenter/newportal/Portal.aspx?pageid=3). For systems that are not in CSI, please review the CSI Application Entry Guide(https://catecollaboration.citigroup.net/entarch/external/Tools%20Support/CSI%20Application%20Entry%20Guide.pdf) and the CSI User Guide (http://catecollaboration.citigroup.net/entarch/external/Tools%20Support/CSI-User-Guide.pdf)
Citi Information Security Standards (CISS)	The connectivity must comply with all requirements in Citi Information Security Standards (CISS).

Choosing Your Connection Type

This program, through Citi Market Place, supports five separate connectivity products. Selecting the appropriate product for your business requirements will ensure proper handling of your request.

Product	Definition	Examples
Firewall Access Request **Click Here to Submit a Firewall Request**	A firewall is network security system that controls the incoming and outgoing network traffic by analyzing the data packets and, based on defined rules, determines whether the traffic should be allowed through or not. Firewalls act as barriers between a trusted, secure internal network and another network (e.g., the Internet, 3rd Party vendor/partner networks) that is not known to be secure and trusted. The risk level of the rules are based on direction (into or out of the Citi network) of IP Addresses of the requested source or destination and the service and protocol being used for the communication.	- An internal trading platform requires a connection to an external third party to execute orders. - Third Party vendor requires access to a development server to perform development work on specific applications. - Third Party Vendor needs access to production apps to perform Customer Service functions from their remote site.
Proxy Change Request **Click Here to Submit a Proxy Request**	A proxy is a server which controls how users can access Internal or Internet Websites. A proxy server acts as an intermediary for requests from a clients/users browser connections seeking resources from other servers. The client browser is configured to use a particular proxy instance. This proxy determines which addresses the user may access.. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server. Proxy	- If Third Party users need access to a Citi Internal web site, such as one-reset, planview, infoman, etc a Proxy Filter/Whitelist request would be submitted for the Proxy Instance used by the third party. -If a group of Citi users need access to a site that is available via a B2B connection then a PAC FILE request would be submitted. The PAC file will ensure that the connectivity goes over

	instances are created for MA&D (Merger, Acquisitions and Divestitures), Third party access and/or restricted user access. There are three separate type of proxy requests reviewed in this section: Filter/Whitelist, PAC File, Proxy Plug or Socks. Proceed to the Proxy section for specific details on each request type.	the B2B link instead of out via the Internet.
Security Access Control List Change Request **Click Here to Submit a SEC ACL Request**	A Security Access Control List (SEC_ACL) provides a separation between network segments within the Citi network or provides a barrier between a third party and the Citi network. SEC_ACL's are applied to router interfaces to restrict access for devices that are **managed** by 3rd Party vendors or to **restrict the connectivity** that is allowed to the devices. SEC_ACL: A network hardware device hosting an access list detailing hosts and/or networks permitted via specific ports, used in lieu of a firewall SEC_ACL Internal: An internal device segregating servers or applications from the internal network.	Vendors that support various devices that are located on the Citi network will have ACLs created that limit the connectivity (IP address, protocol and port) that will be allowed between devices that the vendor manages and other non-managed devices. ACLs will be applied to specific network segments that restrict the connectivity between devices (IP address, protocol and port) and restricted devices such as ATMs will be used to limit risk to those devices.
IP Registration Request **Click Here to Submit an IP Reg Request**	Connectivity allowing remote access to specific devices on the Citi Network via a non-fixed Internet location. Each request is either for Citi Employees or specific Third Parties. Citi Employees belong to a single Access Control List (ACL) and each vendor belongs to their specific ACL. The connectivity between the remote party and the Citi device will utilize the Citi Cisco AnyConnect Secure Mobility Client© via the Internet, creating a secure, encrypted tunnel between the user	Remote Access provides for connectivity via the Internet to a Citi network hardware device hosting an access control list detailing hosts and/or networks permitted via specific ports for each vendor.

	and the Citi destination or network segment.	
	Users will authenticate using a Citi issued Safeword Card to obtain access to the registered destinations.	
Third Party Access AppSense Request [Click Here to Submit an AppSense Request](#)	Third party user access to applications or servers via the Third Party Architecture (TPA) virtualized environment is controlled by Appsense. Appsense creates a user profile that specifies the network application and/or ports the third party user is permitted to access Appsense has a configured blacklist to block access to a specific list of applications and ports. Access to any of the applications or ports on the blacklist must be requested by through the use of this process.	A third party developer needs to utilize ssh (tcp/22) from their TPA device to a server in one of the Citi DMZs. An Appsense request to allow the connectivity between the TPA session for this user and the servers in the DMZ, and the right to use tcp/22 from the TPA to the DMZ server will need to be submitted.

Firewall Access Request

Introduction to Firewall Change Requests

A Firewall facilitates network security through the filtering or blocking of traffic as defined by a set of rules. Firewall rules determine the type of traffic allowed to come into, and out of the network. Properly implemented and maintained firewall rules are an integral part of Citi's Defense in Depth network security strategy.

Part of determining the control requirements around access through the firewall is understanding between which two network resource types that the firewall rule (or change request) is going to allow network traffic to flow. The network resource types are listed below.
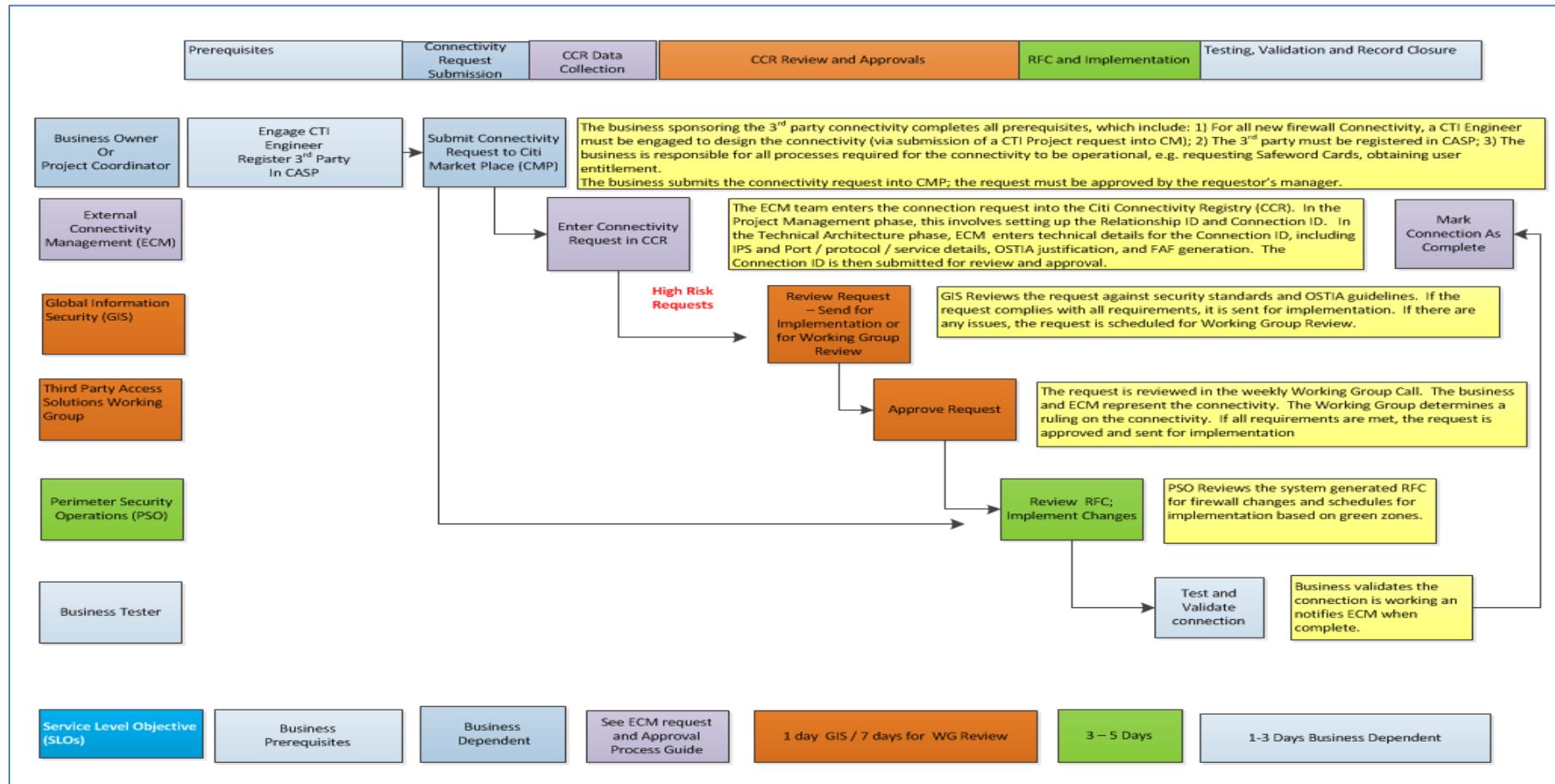
Business to Business (B2B)	Dedicated connection to a third party; B2B establishes a dedicated connection between an outside organization and the Citi network that remains active and available 24/7 by 365 days a year. The dedicated connection results in an "always on" connection.
VPN	A private network established over the Internet connecting remote networks
U-turn	Connections between two outside entities using Citi as a pass through
DMZ	A connection that utilizes the DMZ portion of the network to segregate data due to security requirements.
Citiplex	Segregated segment due to external access or security requirements; may have access to the internet or third parties
Trusted Subsidiary	A connection going to an entity owned by Citi, with systems managed, or partially managed, by Citi. Requires segregation due to location or regulatory requirements
Untrusted Subsidiary	A connection going to an entity owned or acquired by Citi but has not achieved Trusted status.

After understanding the network resource segments involved in the change request, the direction of the traffic between the resource types, the type of traffic (port/protocol/service) and the broadness of the connectivity (how many devices involved) there are considerations in evaluating the risk and control requirements around each change request.

A modification to the current Firewall rule set requires the submission of a change request to the External Connectivity Management team through the use of Citi Market Place. The ECM team works with the business to confirm the requirements of the firewall rule change and ensure its compliance with the current Citi Information Security Standards. Once these requirements have been met the ECM team will submit the request for review, approval and processing. The processing of the request is completed by Perimeter Security Operations (PSO) who is responsible for implementation of the request.
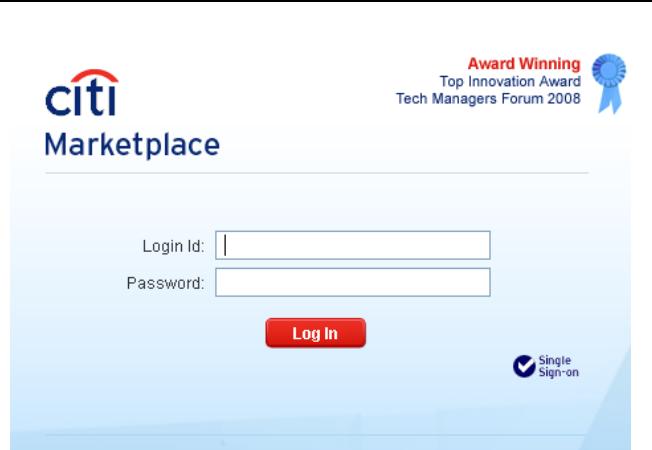
The next section explains the Firewall change request process and workflow. It will assist the business user with completing the perquisites, the marketplace submission process, approval requirements, and connection verification after initial implementation and every 365 days thereafter

Firewall Submission Workflow – New Connectivity

Prerequisites	Connectivity Request Submission	CCR Data Collection	CCR Review and Approvals	RFC and Implementation	Testing, Validation and Record Closure

Business Owner Or Project Coordinator → **Engage CTI Engineer Register 3rd Party In CASP** → **Submit Connectivity Request to Citi Market Place (CMP)**

The business sponsoring the 3rd party connectivity completes all prerequisites, which include: 1) For all new firewall Connectivity, a CTI Engineer must be engaged to design the connectivity (via submission of a CTI Project request into CM); 2) The 3rd party must be registered in CASP; 3) The business is responsible for all processes required for the connectivity to be operational, e.g. requesting Safeword Cards, obtaining user entitlement.
The business submits the connectivity request into CMP; the request must be approved by the requestor's manager.

External Connectivity Management (ECM)

Enter Connectivity Request in CCR

The ECM team enters the connection request into the Citi Connectivity Registry (CCR). In the Project Management phase, this involves setting up the Relationship ID and Connection ID. In the Technical Architecture phase, ECM enters technical details for the Connection ID, including IPS and Port / protocol / service details, OSTIA justification, and FAF generation. The Connection ID is then submitted for review and approval.

Mark Connection As Complete

Global Information Security (GIS)

High Risk Requests

Review Request – Send for Implementation or for Working Group Review

GIS Reviews the request against security standards and OSTIA guidelines. If the request complies with all requirements, it is sent for implementation. If there are any issues, the request is scheduled for Working Group Review.

Third Party Access Solutions Working Group

Approve Request

The request is reviewed in the weekly Working Group Call. The business and ECM represent the connectivity. The Working Group determines a ruling on the connectivity. If all requirements are met, the request is approved and sent for implementation

Perimeter Security Operations (PSO)

Review RFC; Implement Changes

PSO Reviews the system generated RFC for firewall changes and schedules for implementation based on green zones.

Test and Validate connection

Business validates the connection is working an notifies ECM when complete.

Business Tester

Service Level Objective (SLOs)	Business Prerequisites	Business Dependent	See ECM request and Approval Process Guide	1 day GIS / 7 days for WG Review	3 – 5 Days	1-3 Days Business Dependent

Submitting Firewall Access Marketplace Order

The Citi Market Place form required to initiate the request can be accessed by following the below steps

	Log into Citi [Marketplace](https://cmp.nj.ssmb.com/marketplace/control/main) (https://cmp.nj.ssmb.com/marketplace/control/main) using your Single Sign On (SSO) ID.
	Search for *CCR* at the top right hand of the screen
	Select the Citi Connectivity Registry Request form

Alternatively, you may access the form directly via this [link](https://cmp.nj.ssmb.com/marketplace/control/product/~productId=31622_331228_GLOBAL#)
(https://**cmp.nj.ssmb.com/marketplace/control/product/~productId=31622_331228_GLOBAL#**)

Request Type

The CMP form will allow you to request a brand new connectivity or to modify an existing one through a technical update to a Firewall Request. The questionnaire section for both request types require identical information be provided with only a slight exception; a technical update will request the existing CCR ID be provided, so that the specialist assigned can link the modification with the existing ID, while a New Connection does not require this information.

Note: All connectivity requests must be made or approved by a Citi employee

Field	Explanation / Data To Enter
Request Type:	

*Request Type
- New Connection {Creation of Entirely New CCR ID}
- Technical Updates {Existing CCR ID: Add, Modify and/or Delete Rules}
- Non-Technical Update {Existing CCR ID: Add or Remove Contacts}
- Termination {Existing CCR ID: Termination of the entire CCR ID and all rules}
- Assistance Request

Type of Connectivity Involved:	

* Type of Connectivity Involved

Firewall
(Please select)
Firewall
AppSense
Security Access Control List
Proxy
IP Registration

| **Click here to download the Firewall connectivity template. Upload required on tab 4, technical details** | Click here to download the Firewall connectivity template. Upload required on tab 4, technical details. |

Does this request require a proxy change as well?	If **Yes**, select Proxy type that is needed. After selecting the type of Proxy that is needed, you will need to download the template file
Is the connectivity part of an ongoing Merger, Acquisition & Divestiture effort?	
Has CATE Network Engineering been engaged/assigned to this project?	

Request Urgency * **Request Urgency** (Please select) (Please select) BAU Business Critical Emergency	The urgency of your request is determined by the required implementation date and the potential impacts to Citi were the request not implemented. *Note that requests should not be classified as higher than BAU unless there is a justifiable business reason for doing so. **BAU:** Business As usual – Request will follow normal business SLO for implementation, typically 5 to 10 business days. **BUSCRIT:** Business Critical - Request is classified as critical, rush implementation. BUSCRIT requests require answering business critical questions and Managing Director approval. BUSCRIT SLO 3 to 5 business days. **EMER:** Emergency - Requests are classified as an emergency due to a break/fix of a production failure. EMERs require a ticket in ServiceNow, CT, or EMS, an emergency justification and Managing Director approval. **Please Note: Business Critical requests require Managing Director approval. EMERs require MD Approval and an EMS ticket number.)**
Project Sector: * **Project Sector** (Please select) (Please select) Corporate Center CTI GCB ICG	Select the Sector of the business who will own the connectivity.
Project Region: * **Project Region** (Please select) (Please select) ASPAC EMEA JAPAN LATAM North America	Select the region where the Business resides and the majority of the business activity will reside.

Does this connection request require direct access to a destination on the Citi network by a 3rd party other than to receive virtualized PC access (Such as Citrix, VDI, TPA, Sun Global Desktop SOA Gateway)?	Business 2 Business (B2B) establishes a dedicated connection between an outside organization and the Citi network that remains active and available 24/7 by 365 days a year. The dedicated connection results in an "always on" connection. A direct B2B connection can only be used if SOA Gateway, Citrix/VDI, and Sun Global Desktop connectivity options are one or more of the following 1) not cost effective 2) cannot be used or 3) only application connectivity is required. Note that all B2B access requests must go through the OSTIA process identified here.
Please select all of the reasons that this direct connectivity is being used in lieu of a virtualized PC session:	If you must use direct B2B connection, identify the reason(s) why you are unable to use a virtualized connectivity solution. The three available options are the only possible exceptions. If none of these apply, you must use the virtualized connection solution. - Not Cost Effective - Application connectivity is required - A virtualized PC session will not work (Examples of virtualized sessions include; SOA Gateway, Citrix / VDI / Third Party Access (TPA) Sun Global Desktop)
Connectivity Justification **By audit requirement it is critical that you provide sufficient details around the BUSINESS JUSTIFICATION for the connectivity you are requesting.**	All Firewall change request must have business details providing an explanation as to why the connection is required. Please provide a clear and documented benefit to Citi businesses or customers. The connectivity must be legally permissible, have ISO approval and be represented by a Citi Employee. Attempt to provide answers to all of the following questions.. What business processes and owners of these processes are being supported? What systems and or applications are used in this process? Is this a new process or a change to an existing process or service? Please make sure to include Citi SOW number(s) if applicable, any other supporting details. Note: Requests containing insufficient detail will result in delay of processing of the request or cancelation. * All Merger / Acquisitions / Divestitures must have an active Transition Services Agreement (TSA) for all requests..

Business Case

Field	Explanation / Data To Enter
ServiceNow Business CAB Approver Group/Code. Supplying the Business CAB Approver Code may help reduce the number of approvers required.	Please provide a ServiceNow Business CAB RFC Approver Code. Supplying the Business CAB RFC Approver Code may help reduce the number of RFC approvers required.. You can look them up here: RFC CAB Approver Codes . Please select your choice ONLY from the "ID" column
Do not implement before Do not implement before [ ]	Populate with a date when there is potential risk associated to the connection if it were to be implemented prior to a certain date. For example, if a contract between Citi and a Third Party indicates data transfer is not to commence before 5/1/2013, then this date should be provided here.
Requestor - (must be Citi employee/FTE): * Requestor - must be Citi Employee/FTE No Value Set **Update**	Enter the SOEID of the Citi FTE (full time employee) who is requesting connectivity.
Business Owner - Primary (must be Citi employee/FTE): *Business Owner - Primary No Value Set Update	Enter the SOEID of the Citi FTE (full time employee) who will be responsible for connectivity. Note: The Primary business owner will be responsible for providing connectivity details, confirmations, and completion of annual connectivity verification reviews.

<u>Business Owner - Secondary (must be Citi employee/FTE) *Note, the secondary cannot be the same as primary.</u> *Business Owner - Secondary No Value Set Update	Enter the SOEID of the Citi FTE (full time employee) who will be a backup or secondary resource for the connectivity. Note: The Secondary business owner will be able to providing connectivity details, confirmations, and completion of annual connectivity verification reviews.
<u>Project Coordinator (must be Citi employee/FTE):</u> *Project Coordinator No Value Set Update	Enter the SOEID of the individual who is submitting the request on behalf of the business or managing the Connectivity Project. This individual will have no ownership of the connection, but will be utilized as a resource for project and connectivity details.

ISO: *ISO Look Up	Enter the SOEID of the Business Information Security Officer responsible for verifying the business request requirements when needed.. If you do not know the BISO, please contact the business manager for assistance. Otherwise you may use the Locate Your BISO tool located here (http://www.citigroup.net/informationsecurity/locate_biso.htm). An ISO will no longer be notified or required to review/approve new connectivity requests or changes to connectivity requests. You should however be aware that an ISO contact will continue to be collected for every connection request record. You will receive an automated system e-mail notifying you have been selected as an ISO contact for a connection request, and provide you the opportunity to opt out if this selection was made in error. Reasons an ISO contact is required for a connectivity request record are as follows: • In the event that the External Connectivity Analyst needs to contact you about the change requested in the record. • As an escalation point for the Annual Connectivity Verification (ACV) process where the business owner has been unresponsive. • As an escalation point in the Buscrit/EMER or Temporary Approval process where the business owner has been unresponsive. Any ISO (BISO, TISO, or GISO) who supports the business can be selected.
*Business Tester No Value Set Update	Enter the SOEID of the business contact responsible for testing, or coordination of the testing, of the connectivity once it has been implemented. The tester will be listed on the RFC and will be required to provide confirmation of his successful testing. The tester can be the same as the Primary/Secondary owner.

Third Party Details

This section of the Marketplace form is used to obtain information regarding Third Party vendors. The questions will only need to be populated if the response to the first item "Does this request involve a Third Party" is yes.

Field	Explanation / Data To Enter
Who will this request for connectivity service? * Who will this request for connectivity service? (Please select) (Please select) Client, Customer, Partner Vendor, Supplier, Regulatory Agency, Government Agency Internal Users, Internal Connectivity	Select Client, Customer, Partner or vendor, supplier, partner, client, or government agency, these are all considered Third Party. If the destination is not Citi owned, then it is considered a third party.
Vendor Contractual Statement of Work Vendor Contractual Statement of Work Remaining characters: 255	Please provide Statement of Work Tracking ID wherever contract exists to support the connectivity Request.
Third Party Company Name: * Third Party Name	Provide the name of the Third Party organization who will be utilizing the connectivity that requires access through the Firewall

CASP Supplier ID: *CASP Supplier ID [_____]	Enter the CASP [Citi Approved Supplier Program] Supplier number associated with the third party vendor. This information may be obtained by querying the CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp) A CASP Supplier ID must be obtained and entered before a Third Party firewall modification can be processed. If the third party has not been registered in CASP please review the process requirements in the FAQ (https://casp.ny.ssmb.com/casp/popups/file.asp?filename=FAQ.doc&ID=0)
CASP Detail ID: *CASP Detail ID [_____]	Enter the CASP [Citi Approved Supplier Program] Detail ID corresponding to the Supplier and Business relationship. This information may be obtained by querying the CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp) A CASP Detail ID must be obtained and entered before a Third Party firewall modification can be processed. If the third party has not been registered in CASP please review the process requirements in the FAQ (https://casp.ny.ssmb.com/casp/popups/file.asp?filename=FAQ.doc&ID=0)
Third Party Contact Name: * Third Party Contact Name [_____]	Enter the name of the contact person at the Third Party. This information can be obtained from the CASP Procurement Manager listed for the Third Party in CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)
Third Party Contact Type: * Third Party Contact Type (Please select) Relationship Manager Supplier Third Party Contact Technical Support	Select the current role of the contact at the third party.
Third Party Contact Phone: * Third Party Contact Phone [_____]	Enter the phone number of the contact person at the Third Party. This information can be obtained from the CASP Procurement Manager listed for the Third Party in CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)

Third Party Contact E-mail: *** Third Party Contact E-Mail** [ ]	Enter the Email Address of the contact person at the Third Party. This information can be obtained from the CASP Procurement Manager listed for the Third Party in <u>CASP database.</u>(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)

Technical Details

You will be required to upload an excel file with the details of your connection request.

- Download and populate the form located here
  (https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/Bulk%20Upload.xls)
- Upload the document into the CMP form using the appropriate Update section

Please estimate how frequently this connectivity will be used * Please estimate how frequently this connectivity will be used Biweekly (Please select) Daily Weekly Biweekly Monthly Bimonthly Quarterly Semi-Annual Annual As-needed (no set schedule, example: COB)	Select the data frequency

Indicate the type and highest classification of data being accessed with this connectivity. Data must be encrypted end to end if it is Confidential or Higher * Customer Data (Please select) (Please select) Public Internal Confidential Restricted Not Applicable * Citi Data (Please select) (Please select) Public Internal Confidential Restricted Not Applicable	Select the classification that best corresponds to the data that is being transferred. **Confidential:** Information that Citi Businesses are obligated to protect including, but not limited to information belonging to: customers, Workers, Third Parties, or Citi Businesses. Any combination of data subject to regulatory or contractual restrictions on disclosure. Information that the Business determines has the potential to provide a competitive advantage or have a significant impact on the Business if disclosed to unauthorized individuals. **Internal:** Information that is commonly shared within Citi is not intended for distribution outside Citi and is not classified as Restricted or Confidential. **Public:** Information that is freely available outside of Citi or is intended for public use by the Information Owner. **Restricted:** Information that, if disclosed to unauthorized individuals, could have a significant impact on Citi's legal or regulatory obligations or on its financial status, customers or franchise. **N/A:** No Data will be transferred.

The Bulk Upload spreadsheet has recently changed. Please ensure you download and use the new version. Submissions containing the outdated form will result in your request being cancelled, which will cause processing delays.

* Click here to download the connectivity template. Upload the completed template below once finalized.

No Attachment

Update

For guidance on populating the form please review the comments added to the header column of the file

Priority Questions

This section of the Marketplace form is required when the connection urgency has been entered as either *Business Critical* or *Emergency* under section *Project Details*. The added details are required for justifying why the request cannot be entered as *BAU (Business as Usual)*.

Business Critical - Change required to support a Business Critical initiative and mitigate compliance, regulatory, financial or reputational risk or impact. The change is normally associated with a business-driven service enhancement. The change is given priority and resources made available ahead of schedule for change building, testing and implementation. The change follows an expedited review and approval process. Examples: Late files for business conversion; Audit Risk and Review or compliance and control regulatory requirement; Market driven parameter change.

Field	Explanation / Data To Enter
VT (Sev 1-2), ServiceNow or EMS Number *VT (SEV 1-2), ServiceNow or EMS Number	*#Only required for EMERs#* All Firewall submissions with *Request Urgency* of *Emergency* require an associated Virtual Ticket ServiceNow ID or EMS Number. Emergency requests without a valid number will not be processed.
Provide the name/SOE ID of the approving Senior Managing Director *Provide the name/SOE id of the approving Senior Managing Director No Value Set Update	Use the provided search functionality to find the Managing Director who will provide their approval to proceed with the EMER/BUSCRIT request. Note: The search box is limited to Citi employees with MD or higher title.
Which business is requesting the change if different from the group raising the RFC? *Which business is requesting the change if different from the group raising the RFC?	Populate the business following Global Directory formatting standards.

Describe the impact to the Business if this change does not occur out of cycle. *Describe the impact to the Business if this change does not occur out of cycle. |	Explain, in detail, what negative impact would affect the business and/or Citi as a whole if the firewall modification is not made in an expedited fashion. Provide as much detail as possible, including contract deadlines, financial loss amounts, or penalties. This information will be reviewed, and confirmed, to determine whether your request does, in fact, require expedited handling.
What process failed that prevented this change from being able to follow the normal change cycle?. *What process failed that prevented this change request from being able to follow the standard change cycle?	Explain, in detail, why this request was not submitted to the External Connectivity Management team with sufficient time to undergo the normal change cycle. This information will be reviewed, and confirmed, to determine whether your request does, in fact, require expedited handling.
Which department is the owner of this process? *Which department is the owner of this process?	Populate the department following Global Directory formatting standards.
Are there any other changes scheduled during the same time frame for the same or related environment? *Are there any other changes scheduled during the same time frame for the same or related environment? No ▾ (Please select) Yes No	Provide details on known changes that will be occurring during the time frame you are requesting a firewall change be made. Any changes potentially affecting the source or destination networking environments should be noted.
Does any additional business testing need to take place for this unplanned change? *Does any additional Business testing need to take place for this unplanned change? (Provide details) *Remaining characters: 255*	Please note if your business requires testing beyond the normal implementation verification step that will be completed after the firewall change has occurred. Additional business testing can include verification that the destination and source application are compatible and verification that the two applications are running as expected pre-change.

Additional Information

Please assist the processing team by answering the following optional questions to help in expediting your request.

Field	Explanation / Data To Enter
<u>Other Documentation</u>	Use this option to provide any documentation you would like the reviewer to take into consideration. If you have design documentation from a CTI project request, please include it in this section.
<u>Comments</u> **Comments**	Use this space to enter any additional information you would like the reviewer to take into consideration

What to Expect Next

Once the CMP request has been completed, the request will be routed to the External Connectivity Management team and a specialist will be assigned to support the request. The External Connectivity Specialist will review the request details and reach out to the submitter for clarification on any incorrect/outstanding items before transferring the request into the Citi Connectivity Registry. If at any time the External Connectivity team reaches out to the business for additional information and no response is received within 14 days, the CMP may be considered closed.

Certain Firewall requests will be classified as high risk or non-standard; high risk requests are defined as those that require access through a source, destination and port combination that contain known vulnerabilities. These combinations are detailed on the protected excel file located [here](https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/High%20Risk.xlsx)
https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/High%20Risk.xlsx

In order to compensate for the vulnerabilities created by these high risk requests the business will be required to provide information/controls above and beyond that of a regular request.

Type	Action	SLA*
EMER BUSCRIT	**Managing Director Approval** A senior manager, at the Managing Director Level or higher, must approve all requests submitted with urgency of Emergency or Business Critical. The MD approval will be done through resolve it after receipt of an automated email notification generated upon submission of the Citi Market Place request.	Business Dependent. *Historical Median:* 0.2 days
High Risk	OSTIA [Operating System Trust or Interactive Access] Questionnaire OSTIA Questionnaire is required for connectivity requests that a) allows the client machine to directly access the host machine on the Citi internal network at the operating system level or b) allows the target user to have command shell access to the operating system or c) uses any port that is used for non-default services. If the request constitutes as an OSTIA item, you will be required to provide additional information to the ECM [External Connectivity Management] team via email. Click on the header of this section to obtain details on what will be required.	Business Dependent
High Risk Non Standard	**Global Information Security (GIS) Review** Once approved by the business and ECM, the request is routed to GIS for review against security standards and OSTIA guidelines. If the request complies with all requirements, it is sent for implementation. If there are any issues, or the request is deemed a high risk, the request is schedule for Working Group review.	1 day
Requests marked during GIS	**Third Party Working Group Approval** All requests marked for review by GIS Review, require a higher level Third Party Working Group Approval. The Third Party Access Solutions	7 days *Historical Median*:

review	Working Group operates under the direction of the Information Security Risk Operating Committee (ISROC) to review connectivity requests that traverse the Citi perimeter. TPASWG review occurs every Tuesday at 9am ET. The ISO review must be completed and submitted in CCR prior to 12:00 noon ET for the Monday before the Tuesday meeting in order for the request to be added to the agenda of the Working Group meeting.	1.3 days
All	**RFC [Request for Change] Confirmation/Approval** An RFC request will be auto-generated by the CCR once a request has been fully approved by the business, ECM and GIS; and PSO. The business will receive notification of the RFC creation from the PSO team, and through an automated system notification. It then falls upon the business to ensure the RFC defined approval group reviews and approves the RFC in time to meet the identified implementation date. The requestor should ensure the RFC timeline for the change is adequate to meet the business requirement and/or contact PSO if any scheduling updates are needed. Contact PSO directly via email at *GT Global PSO Change Management if there are any concerns about the change. PSO will assist the requestor in understanding how to properly address issue that may arise. Additional details can be found on the PSO user guide (https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/PSO%20Firewall%20Change%20Request%20Guidelines.pdf)	Business Dependent.
All	Connectivity Verification Upon approval of the RFC request, the Primary/Secondary Business Owner [as selected on the original CMP request] will receive an email from the PSO [Perimeter Security Operations] requesting they prepare to verify the connection was successfully implemented. Requestor should notify PSO prior to the day of the change if there are any special testing requirements, like joining a particular audio bridge or providing support during long-duration testing/check out periods. Requestor should notify PSO if they do not plan on testing, and confirm that they accept the risk of the change not work as planned after the change green zone has ended. If the connection works as planned the requestor should notify PSO that the change was tested and that they are satisfied that the connectivity is functioning correctly. If there are implementation errors identified during the green zone, PSO will make the necessary updates and ensure the connection is functioning as planned. Additional details can be found on the PSO user guide (https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/PSO%20Firewall%20Change%20Request%20Guidelines.pdf)	Business Dependent.
All	Annual Connectivity Verification 365 days after the Firewall Implementation the Primary/Secondary Business Owner [as selected on the original CMP request] will receive	Business Dependent 90 Day

	an email requesting they complete the Annual Connectivity Verification. You have 90 days to complete the ACV. If the ACV is not completed it will be reported on the monthly report to Senior Management. Click on the header of this section to obtain additional information.	Max
All	Notifications Business users assigned to the request as Submitter, Information Security Officer, Business Manager, Project Coordinator, and Technical coordinator will receive email notifications when an action is required. Please ensure that you pay special attention to any emails coming from ***OTRM US CCR** or containing **"CCR Notification"** on the subject line. For additional details on the notifications please review the notifications section in the appendix.	N/A

SEC_ACL (Security Access Control List Request)

Introduction to Security Access Control List Requests

A Security Access Control List [SEC_ACL] is, similar in function to a Firewall, intended to restrict access to specific applications for a defined user set; just as with a traditional firewall, access is based on IPs, subnets, protocol, port, and direction. A Security Access Control List can only be deployed in place of a firewall rule when an already deployed router is capable of handling the configuration.

A Security Access Control List [SEC_ACL] request is required to create or update a security control being used in lieu of a traditional firewall. A SEC_ACL will be installed on a router instead of a firewall and all requests therefore follow Network Engineering processes.

Two separate business requests are required to create or update an SEC_ACL.
1. An External Connectivity request to gain approval for the traffic that you want to pass through the ACL.
2. An Engineering request to identify and configure the routers that the ACL is applied to.
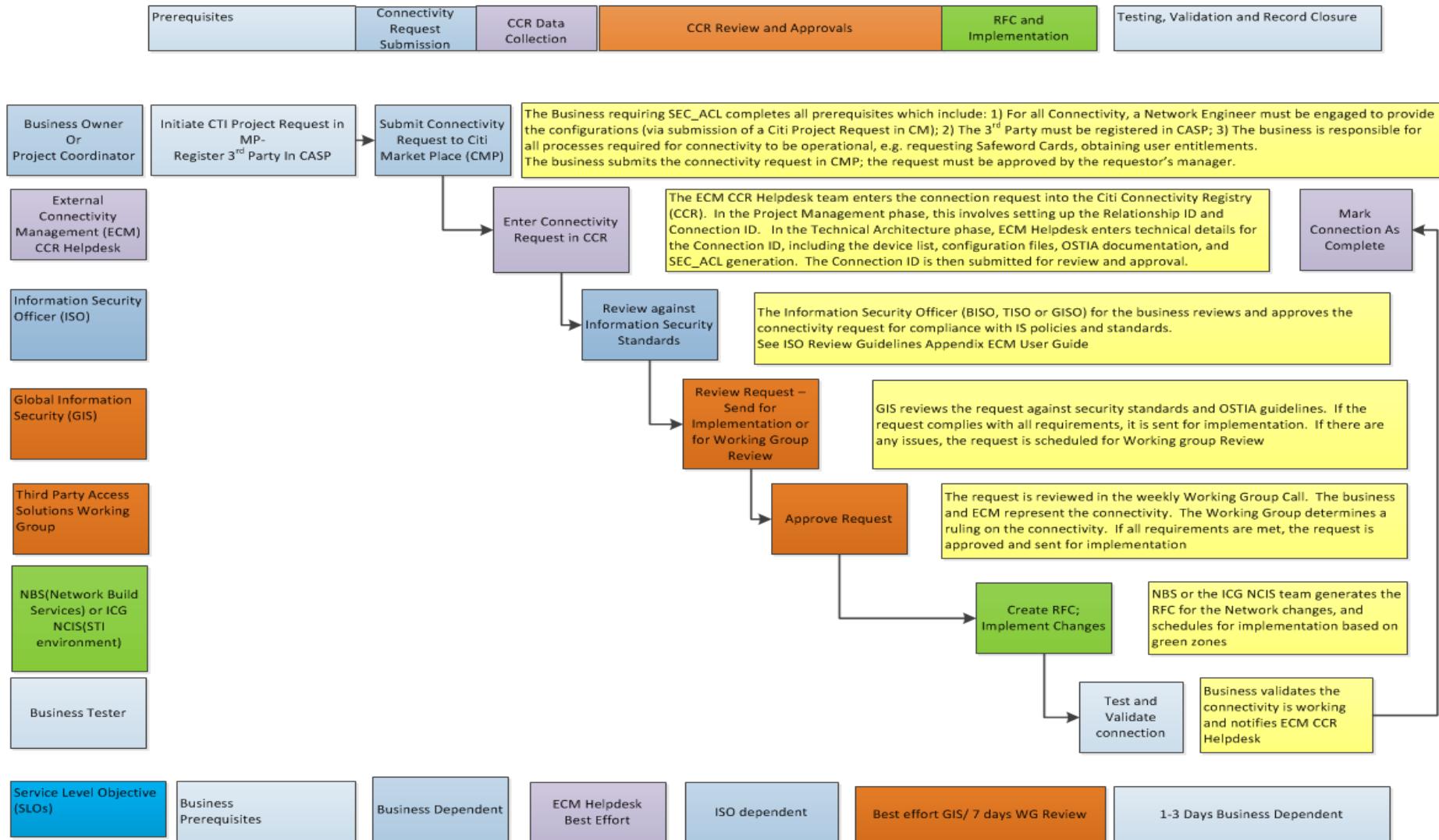
Each of these are independent requests, and **_BOTH_** must be completed. The completed Engineering request, and outcome, should be attached to the ECM request. (

Important information for SEC-ACL Modifications

If the existing SEC-ACL DOES "NOT" have a CCR record because it was created before the SEC_ACL process was implemented in May 2012, you must create a new SEC_ACL record request in CMP for the entire SEC_ACL including the current modifications required.

If the existing SEC_ACL "DOES" have a CCR record, then you need to identify that CCR record # when you submit the CMP request.

Security Access Control List Workflow

| Prerequisites | Connectivity Request Submission | CCR Data Collection | CCR Review and Approvals | RFC and Implementation | Testing, Validation and Record Closure |

Business Owner Or Project Coordinator
Initiate CTI Project Request in MP- Register 3rd Party In CASP → Submit Connectivity Request to Citi Market Place (CMP)

The Business requiring SEC_ACL completes all prerequisites which include: 1) For all Connectivity, a Network Engineer must be engaged to provide the configurations (via submission of a Citi Project Request in CM); 2) The 3rd Party must be registered in CASP; 3) The business is responsible for all processes required for connectivity to be operational, e.g. requesting Safeword Cards, obtaining user entitlements. The business submits the connectivity request in CMP; the request must be approved by the requestor's manager.

External Connectivity Management (ECM) CCR Helpdesk
Enter Connectivity Request in CCR

The ECM CCR Helpdesk team enters the connection request into the Citi Connectivity Registry (CCR). In the Project Management phase, this involves setting up the Relationship ID and Connection ID. In the Technical Architecture phase, ECM Helpdesk enters technical details for the Connection ID, including the device list, configuration files, OSTIA documentation, and SEC_ACL generation. The Connection ID is then submitted for review and approval.

Mark Connection As Complete

Information Security Officer (ISO)
Review against Information Security Standards

The Information Security Officer (BISO, TISO or GISO) for the business reviews and approves the connectivity request for compliance with IS policies and standards.
See ISO Review Guidelines Appendix ECM User Guide

Global Information Security (GIS)
Review Request – Send for Implementation or for Working Group Review

GIS reviews the request against security standards and OSTIA guidelines. If the request complies with all requirements, it is sent for implementation. If there are any issues, the request is scheduled for Working group Review

Third Party Access Solutions Working Group
Approve Request

The request is reviewed in the weekly Working Group Call. The business and ECM represent the connectivity. The Working Group determines a ruling on the connectivity. If all requirements are met, the request is approved and sent for implementation

NBS(Network Build Services) or ICG NCIS(STI environment)
Create RFC; Implement Changes

NBS or the ICG NCIS team generates the RFC for the Network changes, and schedules for implementation based on green zones

Business Tester
Test and Validate connection

Business validates the connectivity is working and notifies ECM CCR Helpdesk

| Service Level Objective (SLOs) | Business Prerequisites | Business Dependent | ECM Helpdesk Best Effort | ISO dependent | Best effort GIS/ 7 days WG Review | 1-3 Days Business Dependent |

SEC_ACL: How to complete the Request:

All Security Access Control List (SEC_ACL) requests require the engagement of a Network Engineer. The assigned Engineer will provide the SEC_ ACL configurations required for security review and approval. To engage a Network Engineer follow these steps

Obtain and populate the latest Network Design Document

1. Click here (https://globalconsumer.collaborationtools.consumer.citigroup.net/sites/NA_NIS/processes/Pages/Initiation_ProjectEngagement.aspx) to be redirected to the Network Engineering Project Engagement site.

2. Once there please click on "Show all items"

3. Scroll down to "Do you need to make minor software Move-Add-Change (MAC) to the existing network/voice infrastructure?"

4. Follow the instructions and download the latest Networks Design Document

5. Populate all fields on the *Base Scope* tab. If you require assistance you may review the *Help* tab on the Networks Design Document or contact the Applied Engineering team at **"*GT GLOBAL Service Engagement**
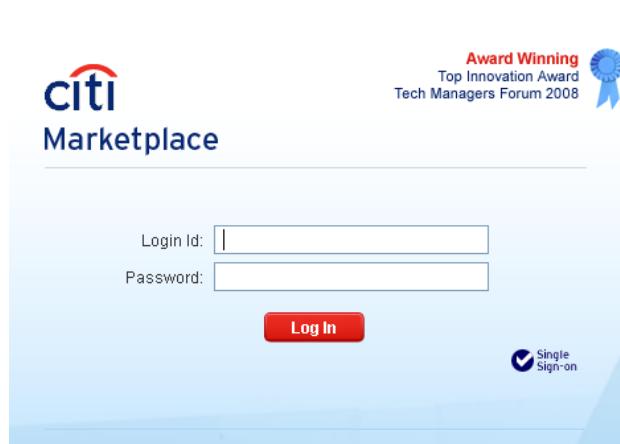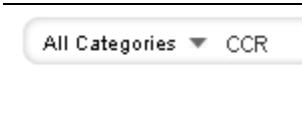
Submit CMP Request

Once you have populated the Network Design Document with accurate information you can proceed to engage Engineering

1. Click here (https://cmp.nj.ssmb.com/marketplace/control/product/~productId=47306_21653_GLOBAL) to be directed to the CTI Project Request Document

2. If you require assistance populating the requested information you may refer to the Marketplace Project Request instructions (https://globalconsumer.collaborationtools.consumer.citigroup.net/sites/NA_NIS/Shared%20Documents/Requestor%20Overview%20November%202014.docx)

3. Attached the Network Design Document

4. Once the above actions have been completed, and you have received the SEC_ACL configurations from the assigned network engineer, proceed to the "Submit SEC_ACL Marketplace Order" to engage the CCR helpdesk and start the risk review process.

Submitting Sec_ACL Change Request

Once you have completed the prerequisites and engaged CATE engineering, you are ready to submit the change request. The Security Access Control Citi Market Place form, required for the SEC ACL Request, can be found by following the below steps

	Log into Citi Marketplace (https://cmp.nj.ssmb.com/marketplace/control/main) using your Single Sign On (SSO) ID.
	Search for *CCR* at the top right hand of the screen
	Select the Citi Connectivity Registry Request form

Alternatively, you may access the form directly via this link
(https://cmp.nj.ssmb.com/marketplace/control/product/~productId=31622_331228_GLOBAL#)

Request Type

The CMP form will allow you to request a brand new connectivity or to modify an existing one through a technical update to a Firewall Request. The questionnaire section for both request types require identical information be provided with only slight exception. A technical update will request the existing CCR ID be provided, so that the specialist assigned can link the modification with the existing ID, wile a New Connection does not require this information.

Field	Explanation / Data To Enter

Request Type:

*Request Type

- ○ New Connection {Creation of Entirely New CCR ID}
- ○ Technical Updates {Existing CCR ID: Add, Modify and/or Delete Rules}
- ○ Non-Technical Update {Existing CCR ID: Add or Remove Contacts}
- ○ Termination {Existing CCR ID: Termination of the entire CCR ID and all rules}
- ○ Assistance Request

Type of Connectivity Involved:

*Type of Connectivity Involved

Security Access Control List

(Please select)
Firewall
AppSense
Security Access Control List
Proxy
IP Registration

All Security Access Control List (SEC ACL) requests require the engagement of a Network Engineer. The assigned Engineer will provide the SEC ACL configurations required for security review and approval. If you have problems attaching your document, or more than one document to attach, please include them in a ZIP file.

To engage a Network Engineer, please click here

(https://catecollaboration.citigroup.net/domains/networks/processes/Pages/Initiation_ProjectEngagement.aspx)**to be redirected to the Network Engineering Project Engagement site. Once there please click on Show all items and follow the instructions under the "Do you need to make a minor software Move-Add-Change (MAC) to the existing network/voice infrastructure?" option. You will need to open an additional MP request and attach the required Network Design Document (NDD). Once the above actions have been completed, and you have received the SEC_ACL configurations from the assigned network engineer, please finish completing this request to engage the CCR helpdesk and start the risk review process.**

Please identify the Market Place request number submitted through the Network Engineering Project Engagement site	Enter the CMP ID for the request submitted as per the above requirement
Please provide any additional SEC ACL Documentation you may have	Attach any additional SEC ACL document you might have.
Please provide any additional SEC ACL Documentation you may have (2)	Attach any additional SEC ACL document you might have.
Please provide the project request number submitted for the Engineer engagement (VPR, TP, CMP)	Provide the VPR, TP, CMP Number
*ACL Was Engineered By No Value Set Update	Use the lookup functionality to select the individual that has engineered the ACL request. This information would be in the Network Engineering Project listed above
*ACL will be integrated by No Value Set Update	Use the lookup functionality to select the individual that integrate the ACL request. This information would be in the Network Engineering Project listed above.

*Request Urgency (Please select) (Please select) BAU Business Critical Emergency	The urgency of your request is determined by the required implementation date and the potential impacts to Citi were the request not implemented. *Note that requests should not be classified as higher than BAU unless there is a justifiable business reason for doing so. **BAU:** Business As usual – Request will follow normal business SLO for implementation, typically 5 to 10 business days. **BUSCRIT:** Business Critical - Request is classified as critical, rush implementation. BUSCRIT requests require answering business critical questions and Managing Director approval. BUSCRIT SLO 3 to 5 business days. **EMER:** Emergency - Requests are classified as an emergency due to a break/fix of a production failure. EMERs require a ticket in ServiceNow, CT, or EMS, an emergency justification and Managing Director approval. **Please Note: Business Critical requests require Managing Director approval. EMERs require MD Approval and an EMS ticket number.)**
Project Sector: * Project Sector (Please select) (Please select) Corporate Center CTI GCB ICG	Select the Sector of the business who will own the connectivity.
Project Region: * Project Region (Please select) (Please select) ASPAC EMEA JAPAN LATAM North America	Select the region where the Business resides and the majority of the business activity will reside.

| Connectivity Justification

By audit requirement it is critical that you provide sufficient details around the BUSINESS JUSTIFICATION for the connectivity you are requesting. | All change request must have business details providing an explanation as to why the connection is required. Please provide a clear and documented benefit to Citi businesses or customers. The connectivity must be legally permissible, have ISO approval and be represented by a Citi Employee.

Attempt to provide answers to all of the following questions..

What business processes and owners of these processes are being supported?
What systems and or applications are used in this process?
Is this a new process or a change to an existing process or service?
Please make sure to include Citi SOW number(s) if applicable, any other supporting details.

Note: Requests containing insufficient detail will result in delay of processing of the request or cancelation.

* All Merger / Acquisitions / Divestitures must have an active Transition Services Agreement (TSA) for all requests.. |

Business Case

Field	Explanation / Data To Enter
Indicate Classification of Data Accessed Indicate Classification of Data Accessed (Please select) (Please select) Restricted Confidential Internal Public Not Applicable	Select the classification that best corresponds to the data that is being transferred. **Confidential:** Information that Citi Businesses are obligated to protect including, but not limited to information belonging to: customers, Workers, Third Parties, or Citi Businesses. Any combination of data subject to regulatory or contractual restrictions on disclosure. Information that the Business determines has the potential to provide a competitive advantage or have a significant impact on the Business if disclosed to unauthorized individuals. **Internal:** Information that is commonly shared within Citi is not intended for distribution outside Citi and is not classified as Restricted or Confidential. **Public:** Information that is freely available outside of Citi or is intended for public use by the Information Owner. **Restricted:** Information that, if disclosed to unauthorized individuals, could have a significant impact on Citi's legal or regulatory obligations or on its financial status, customers or franchise. **Not Applicable:** No Data will be transferred.
ServiceNow Business CAB Approver Group/Code. Supplying the Business CAB Approver Code may help reduce the number of approvers required..	Please provide a ServiceNow Business CAB RFC Approver Code. Supplying the Business CAB RFC Approver Code may help reduce the number of RFC approvers required.. You can look them up here: RFC CAB Approver Codes . Please select your choice ONLY from the "ID" column
Do not implement before Do not implement before	Populate with a date when there is potential risk associated to the connection if it were to be implemented prior to a certain date. For example, if a contract between Citi and a Third Party indicates data transfer is not to commence before 5/1/2013, then this date should be provided here.

Requestor - (must be Citi employee/FTE): * Requestor - must be Citi Employee/FTE No Value Set **Update**	Enter the SOEID of the Citi FTE (full time employee) who is requesting connectivity.
Business Owner-Primary: *Business Owner - Primary No Value Set Update	Enter the SOEID of the Citi FTE (full time employee) who will be responsible for connectivity. Note: The Primary business owner will be responsible for providing connectivity details, confirmations, and completion of annual connectivity verification reviews.
Business Owner-Secondary: *Business Owner - Secondary No Value Set Update	Enter the SOEID of the Citi FTE (full time employee) who will be a back up or secondary resource for the connectivity. Note: The Secondary business owner will be able to providing connectivity details, confirmations, and completion of annual connectivity verification reviews.
Project Coordinator (must be Citi employee/FTE) ***Project Coordinator** No Value Set Update	Enter the SOEID of the individual who is submitting the request on behalf of the business or managing the Connectivity Project. This individual will have no ownership of the connection, but will be utilized as a resource for project and connectivity details.

ISO: *ISO Look Up	Enter the SOEID of the Business Information Security Officer responsible for verifying the business request requirements when needed.. If you do not know the BISO, please contact the business manager for assistance. Otherwise you may use the Locate Your BISO tool located here (http://www.citigroup.net/informationsecurity/locate_biso.htm). An ISO will no longer be notified or required to review/approve new connectivity requests or changes to connectivity requests. You should however be aware that an ISO contact will continue to be collected for every connection request record. You will receive an automated system e-mail notifying you have been selected as an ISO contact for a connection request, and provide you the opportunity to opt out if this selection was made in error. Reasons an ISO contact is required for a connectivity request record are as follows: - In the event that the External Connectivity Analyst needs to contact you about the change requested in the record. - As an escalation point for the Annual Connectivity Verification (ACV) process where the business owner has been unresponsive. - As an escalation point in the Buscrit/EMER or Temporary Approval process where the business owner has been unresponsive. Any ISO (BISO, TISO, or GISO) who supports the business can be selected.
Business Tester: *Business Tester No Value Set Update	Enter the SOEID of the business contact responsible for testing, or coordination of the testing, of the connectivity once it has been implemented. The tester will be listed on the RFC and will be required to provide confirmation of his successful testing. The tester can be the same as the Primary/Secondary owner.
Managing Director * Managing Director No Value Set **Update**	Use the provided search functionality to find the Managing Director who will provide their approval to proceed with the EMER/BUSCRIT request. Note: The search box is limited to Citi employees with MD or higher title.

Third Party Details

This section of the Marketplace form is used to obtain information regarding Third Party vendors where applicable. The questions will only need to be answered if the response to the first item "Does this request involve a Third Party" is: Yes.

Field	Explanation / Data To Enter
Who will this request for connectivity service? *Who will this request for connectivity service? (Please select) (Please select) Client, Customer, Partner Vendor, Supplier, Regulatory Agency, Government Agency Internal Users, Internal Connectivity	Select Client, Customer, Partner or vendor, supplier, partner, client, or government agency, these are all considered Third Party. If the destination is not Citi owned, then it is considered a third party.
Is this request for connectivity servicing a customer, client or partner? *Is this request for connectivity servicing a customer, client or partner? Yes (Please select) Yes No	Select whether the Third Party involved in the request is a current customer or client of Citigroup.
Vendor Contractual SOW: Vendor Contractual SOW Remaining characters: 255	Enter the Vendor contractual Statement of Work (SOW) number associated with the connectivity request. This will be used for review of the project details, connectivity tracking, and Entitlement reviews.
Please upload vendor documentation outlining the traffic flow and/or how the application works.	Please obtain, and upload, Vendor documentation detailing in detail how the proposed connectivity traffic flow would occur. This allows the reviewing team the ability to ensure the proposed plan is accurate and acceptable as per Citi standards.

Third Party Company Name: * Third Party Name	Provide the name of the Third Party organization who will be utilizing the connectivity that requires access through the Firewall
CASP Supplier ID: *CASP Supplier ID	Enter the CASP [Citi Approved Supplier Program] Supplier number associated with the third party vendor. This information may be obtained by querying the CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp) A CASP Supplier ID must be obtained and entered before a Third Party firewall modification can be processed. If the third party has not been registered in CASP please review the process requirements in the FAQ (https://casp.ny.ssmb.com/casp/popups/file.asp?filename=FAQ.doc&ID=0)
CASP Detail ID: *CASP Detail ID	Enter the CASP [Citi Approved Supplier Program] Detail ID corresponding to the Supplier and Business relationship. This information may be obtained by querying the CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp) A CASP Detail ID must be obtained and entered before a Third Party firewall modification can be processed. If the third party has not been registered in CASP please review the process requirements in the FAQ (https://casp.ny.ssmb.com/casp/popups/file.asp?filename=FAQ.doc&ID=0)
Third Party Contact Name: * Third Party Contact Name	Enter the name of the contact person at the Third Party. This information can be obtained from the CASP Procurement Manager listed for the Third Party in CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)
Third Party Contact Type: * Third Party Contact Type (Please select) Relationship Manager Supplier Third Party Contact Technical Support	Select the current role of the contact at the third party.

Third Party Contact Phone: * Third Party Contact Phone	Enter the phone number of the contact person at the Third Party. This information can be obtained from the CASP Procurement Manager listed for the Third Party in CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)
Third Party Contact E-mail: * Third Party Contact E-Mail	Enter the Email Address of the contact person at the Third Party. This information can be obtained from the CASP Procurement Manager listed for the Third Party in CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)

Technical Details

Please estimate how frequently this connectivity will be used * Please estimate how frequently this connectivity will be used Biweekly (Please select) Daily Weekly Biweekly Monthly Bimonthly Quarterly Semi-Annual Annual As-needed (no set schedule, example: COB)	Select the data frequency
Indicate the type and highest classification of data being accessed with this connectivity. Data must be encrypted end to end if it is Confidential or Higher * Customer Data (Please select) (Please select) Public Internal Confidential Restricted Not Applicable * Citi Data (Please select) (Please select) Public Internal Confidential Restricted Not Applicable	Select the classification that best corresponds to the data that is being transferred. **Confidential:** Information that Citi Businesses are obligated to protect including, but not limited to information belonging to: customers, Workers, Third Parties, or Citi Businesses. Any combination of data subject to regulatory or contractual restrictions on disclosure. Information that the Business determines has the potential to provide a competitive advantage or have a significant impact on the Business if disclosed to unauthorized individuals. **Internal:** Information that is commonly shared within Citi is not intended for distribution outside Citi and is not classified as Restricted or Confidential. **Public:** Information that is freely available outside of Citi or is intended for public use by the Information Owner. **Restricted:** Information that, if disclosed to unauthorized individuals, could have a significant impact on Citi's legal or regulatory obligations or on its financial status, customers or franchise. **N/A:** No Data will be transferred.

Priority Questions

This section of the Marketplace form is required when the connection urgency has been entered as either *Business Critical* or *Emergency* under section *Project Details*. The purpose is to obtain an understanding/justification of why the request cannot be entered as *BAU (Business as Usual)* and the corresponding required Managing Director approval information.

The questions will only need to be populated if the request is not BAU (Business as Usual) as per your selection in the *Project Details* section.

Field	Explanation / Data To Enter
VT (Sev 1-2), ServiceNow or EMS Number *VT (SEV 1-2), ServiceNow or EMS Number	*#Only required for EMERs#* All Firewall submissions with *Request Urgency* of *Emergency* require an associated Virtual Ticket ServiceNow ID or EMS Number. Emergency requests without a valid number will not be processed.
Provide the name/SOE ID of the approving Senior Managing Director *Provide the name/SOE id of the approving Senior Managing Director No Value Set Update	Use the provided search functionality to find the Managing Director who will provide their approval to proceed with the EMER/BUSCRIT request. Note: The search box is limited to Citi employees with MD or higher title.
What business is requesting the change? *Which business is requesting the change if different from the group raising the RFC?	Populate the business following Global Directory formatting standards.

Describe the business impact if the change does not occur out of cycle. *Describe the impact to the Business if this change does not occur out of cycle. |	Explain, in detail, what negative impact would affect the business and/or Citi as a whole if the firewall modification is not made in an expedited fashion. Provide as much detail as possible, including contract deadlines, financial loss amounts, or penalties. This information will be reviewed, and confirmed, to determine whether your request does, in fact, require expedited handling.
Does any additional business testing need to take place for this unplanned change? *Does any additional Business testing need to take place for this unplanned change? (Provide details) Remaining characters: 255	Please note if your business requires testing beyond the normal implementation verification step that will be completed after the firewall change has occurred. Additional business testing can include verification that the destination and source application are compatible and verification that the two applications are running as expected pre-change.
What process failed that prevented this change from being able to follow the normal change cycle?. *What process failed that prevented this change request from being able to follow the standard change cycle?	Explain, in detail, why this request was not submitted to the External Connectivity Management team with sufficient time to undergo the normal change cycle. This information will be reviewed, and confirmed, to determine whether your request does, in fact, require expedited handling.
What other changes, if any, are scheduled during the same time frame? *What other changes, if any, are scheduled during the same time frame for the same or a related environment that may clash with this request? (Provide details)	Provide details on known changes that will be occurring during the time frame you are requesting a firewall change be made. Any changes potentially affecting the source or destination networking environments should be noted.
Which department is the owner of this process? *Which department is the owner of this process?	Populate the department following Global Directory formatting standards.

Additional Information

Please assist the processing team by answering the following optional questions to help in expediting your request.

Field	Explanation / Data To Enter
Other Documentation	Use this option to provide any documentation you would like the reviewer to take into consideration
Comments **Comments**	Use this space to enter any additional information you would like the reviewer to take into consideration.

What to Expect Next

Once the CMP request has been completed, the request will be routed to the CCR Helpdesk team and a specialist will be assigned to manage the request. The CCR Helpdesk Specialist will review the request details and reach out to the submitter for clarification on any incorrect/outstanding items before transferring the request into the Citi Connectivity Registry. If at any time the CCR Helpdesk team reaches out to the business for additional information and no response is received within 14 days, the CMP request will be cancelled.

In order to compensate for the vulnerabilities created by requests determined to be high risk, the business will be required to provide additional information including information on controls.

Type	Explanation / Data To Enter	
EMER BUSCRIT	**Managing Director Approval** A senior manager, at the Managing Director Level or higher, must approve all requests submitted with urgency of Emergency or Business Critical. The MD approval will be done through resolve it after receipt of an automated email notification generated upon submission of the Citi Market Place request.	Business Dependent. *Historical Median:* 0.2 days
High Risk Non Standard	**Global Information Security (GIS) Review** Once approved by the business and CCR Helpdesk , the request is routed to GIS for review against security standards. If the request complies with all requirements, it is sent for implementation. If there are any issues, or the request is deemed a high risk, the request is schedule for Working Group review.	1 day
Requests marked during GIS review	**Third Party Working Group Approval** All requests marked for review by GIS Review, require a higher level Third Party Working Group Approval. The Third Party Access Solutions Working Group operates under the direction of the Information Security Risk Operating Committee (ISROC) to review connectivity requests that traverse the Citi perimeter. TPASWG review happens every Tuesday at 9am ET. Cutoff for each week's review is Monday 12 noon ET for ISO approval completion.	7 days *Historical Median*: 1.3 days
All	**Security Engineering Review** All Sec ACL request are reviewed by the Security Engineering team. All	Business Dependent.

|		
	appropriate documents uploaded to the request are reviewed	
All	**Connectivity Verification** Upon approval and implementation the Primary/Secondary Business Owner [as selected on the original CMP request] will receive an email from the GNO [Global Network Operations] requesting they prepare to verify the connection was successfully implemented. Requestor should notify GNO prior to the day of the change if there are any special testing requirements, including how GNO should contact the testers during the test period providing support during long-duration testing/check out periods, or other testing requirements Requestor should notify GNO if they do not plan on testing, and confirm that they accept the risk of the change not work as planned after the change green zone has ended. If the connection works as planned the requestor should notify GNO that the change was tested and that they are satisfied that the connectivity is functioning correctly.	Business Dependent.
All	**Annual Connectivity Verification** 365 days after the SEC ACL Implementation the Primary/Secondary Business Owner [as selected on the original CMP request] will receive an email requesting they complete the Annual Connectivity Verification. You have 90 days to complete the ACV. If the ACV is not completed it will be reported on the monthly report to Senior Management. Click on the header of this section to obtain additional information.	Business Dependent 90 Day Max
All	Notifications Business users assigned to the request as Submitter, Information Security Officer, Business Manager, Project Coordinator, and Technical coordinator will receive email notifications when an action is required. Please ensure that you pay special attention to any emails coming from ***OTRM US CCR** or containing **"CCR Notification"** on the subject line. For additional details on the notifications please review the Notifications Section in the appendix	N/A

Proxy Request
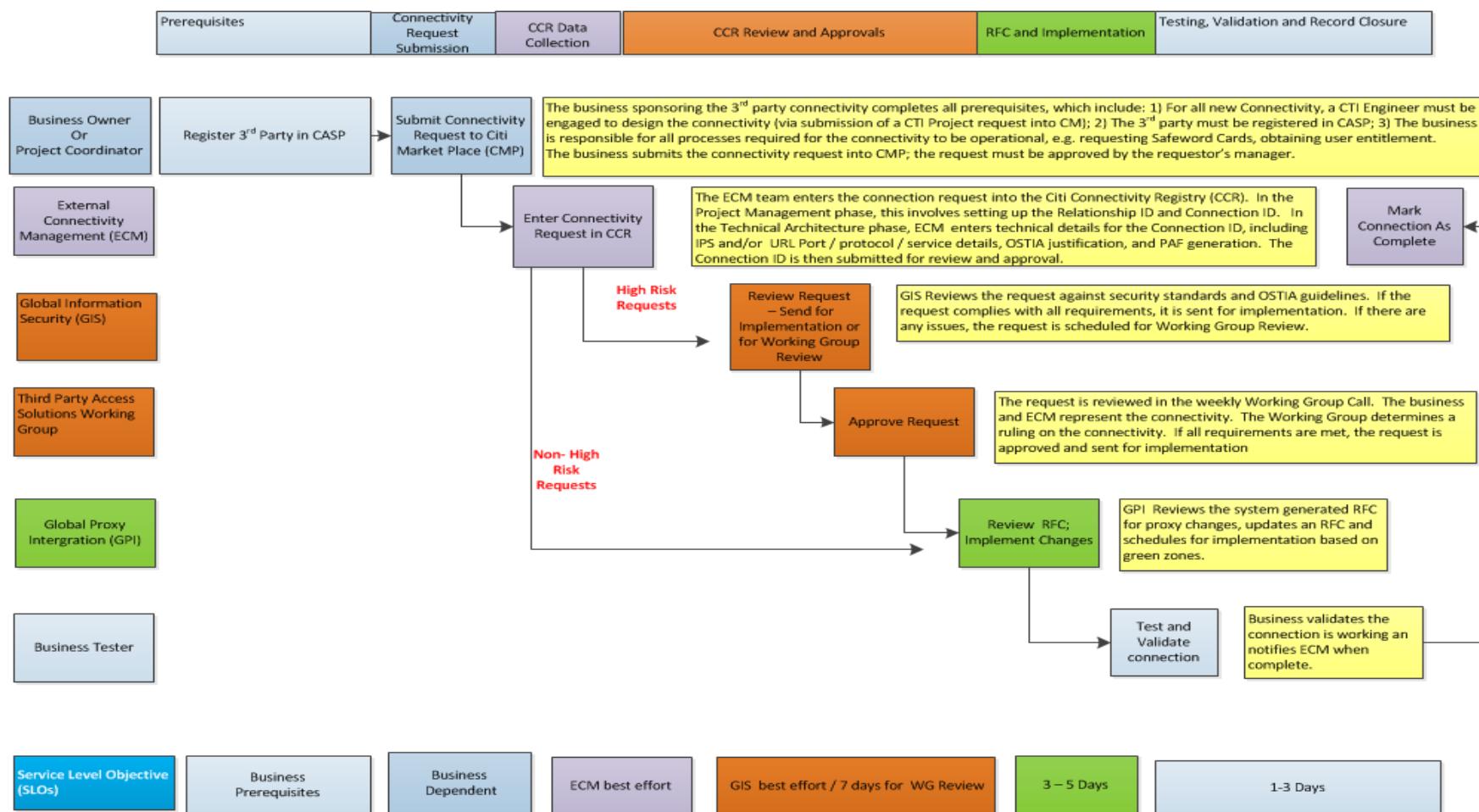
Introduction to Proxy Requests

Described below are the different types of proxies and their corresponding change processes, and the information required to complete a proxy access request submission.

All communication via a proxy must follow the restrictions/requirements defined in the [Prerequisites Section of this document](#) including High Risk / Operating System Trust and Interactive Access (OSTIA) requirements. In addition, any encryption services provided by a proxy are not considered "end-to-end" encryption. Each service run through a proxy must ensure that it is compliant with all Citi encryption standards as listed on the latest CISS.

Proxy Connectivity Request Workflow

Prerequisites	Connectivity Request Submission	CCR Data Collection	CCR Review and Approvals	RFC and Implementation	Testing, Validation and Record Closure

Business Owner Or Project Coordinator → **Register 3rd Party in CASP** → **Submit Connectivity Request to Citi Market Place (CMP)**

The business sponsoring the 3rd party connectivity completes all prerequisites, which include: 1) For all new Connectivity, a CTI Engineer must be engaged to design the connectivity (via submission of a CTI Project request into CM); 2) The 3rd party must be registered in CASP; 3) The business is responsible for all processes required for the connectivity to be operational, e.g. requesting Safeword Cards, obtaining user entitlement. The business submits the connectivity request into CMP; the request must be approved by the requestor's manager.

External Connectivity Management (ECM)

Enter Connectivity Request in CCR

The ECM team enters the connection request into the Citi Connectivity Registry (CCR). In the Project Management phase, this involves setting up the Relationship ID and Connection ID. In the Technical Architecture phase, ECM enters technical details for the Connection ID, including IPS and/or URL Port / protocol / service details, OSTIA justification, and PAF generation. The Connection ID is then submitted for review and approval.

Mark Connection As Complete

Global Information Security (GIS)

High Risk Requests

Review Request – Send for Implementation or for Working Group Review

GIS Reviews the request against security standards and OSTIA guidelines. If the request complies with all requirements, it is sent for implementation. If there are any issues, the request is scheduled for Working Group Review.

Third Party Access Solutions Working Group

Approve Request

The request is reviewed in the weekly Working Group Call. The business and ECM represent the connectivity. The Working Group determines a ruling on the connectivity. If all requirements are met, the request is approved and sent for implementation

Non- High Risk Requests

Global Proxy Intergration (GPI)

Review RFC; Implement Changes

GPI Reviews the system generated RFC for proxy changes, updates an RFC and schedules for implementation based on green zones.

Test and Validate connection

Business validates the connection is working an notifies ECM when complete.

Business Tester

Service Level Objective (SLOs)	Business Prerequisites	Business Dependent	ECM best effort	GIS best effort / 7 days for WG Review	3 – 5 Days	1-3 Days

Submitting Proxy Change Request Marketplace Order

Request Type

The CMP form will allow you to request a brand new connectivity or to modify an existing one through a technical update to a Firewall Request. The questionnaire section for both request types require identical information be provided with only a slight exception; a technical update will request the existing CCR ID be provided, so that the specialist assigned can link the modification with the existing ID,

	Log into Citi Marketplace (https://cmp.nj.ssmb.com/marketplace/control/main) using your Single Sign On (SSO) ID.
  Alternatively, you may access the form directly via this link (https://cmp.nj.ssmb.com/marketplace/control/product/~productId=31622_331228_GLOBAL#)	Search for *CCR* at the top right hand of the screen
	Select the Citi Connectivity Registry Request form

while a New Connection does not require this information.

Field	Explanation / Data To Enter

Request Type:

Type of Connectivity Involved:

Does this request require a Firewall change as well?	
	If you select YES, you will need to downloand the Firewall connectivity template Click **here** to download the Firewall connectivity template. Upload required o technical details.

*Proxy Type (Please select) **(Please select)** Filter/Whitelist PAC File Plug SOCKS New Proxy Instance Free URL List	Refer to the Proxy definitions at the beginning of this section for guidance on which request type best corresponds to your situation.
	Click **here** to download the connectivity template. Upload required on tab 4, technical details. https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/Proxy%20Filter.xlsx
Proxy Type = Plug or SOCKS	**CitiSFT is the preferred connectivity method. Please review the CitiSFT guides available HERE to determine whether CitiSFT will meet your needs .**
Proxy Type = Plug or SOCKS	**Can CitiSFT be used in lieu of plug or socks?** Yes (Please select) Yes No If, after reviewing the CitiSFT guides, you determine that it meets your connectivity requirements select Yes. This will terminate this request and you will need to submit a CitiSFT request following the guides HERE If a CitiSFT does not meet your requirements, select No and be prepared to provide proper justification.
Has CATE Network Engineering been engaged/assigned to this project?	*** Has CATE Network Engineering been engaged/assigned to this project?** (Please select) Yes No If you select YES, you will need to provide the engineers name that you worked with. *** Please provide the Name of the Engineer and the associated project request number (VPR, TP, CMP)** *Remaining characters: 255*

Request Urgency ***Request Urgency** (Please select) (Please select) BAU Business Critical Emergency	The urgency of your request is determined by the required implementation date and the potential impacts to Citi were the request not implemented. *Note that requests should not be classified as higher than BAU unless there is a justifiable business reason for doing so. **BAU:** Business As usual – Request will follow normal business SLO for implementation, typically 5 to 10 business days. **BUSCRIT:** Business Critical - Request is classified as critical, rush implementation. BUSCRIT requests require answering business critical questions and Managing Director approval. BUSCRIT SLO 3 to 5 business days. **EMER:** Emergency - Requests are classified as an emergency due to a break/fix of a production failure. EMERs require a ticket in ServiceNow, CT, or EMS, an emergency justification and Managing Director approval. **Please Note: Business Critical requests require Managing Director approval. EMERs require MD Approval and an EMS ticket number.)**
Project Sector: *** Project Sector** (Please select) (Please select) Corporate Center CTI GCB ICG	Select the Sector of the business who will own the connectivity.
Project Region: *** Project Region** (Please select) (Please select) ASPAC EMEA JAPAN LATAM North America	Select the region where the Business resides and the majority of the business activity will reside.

Does this connection request require direct access to a destination on the Citi network by a 3rd party other than to receive virtualized PC access (Such as Citrix, VDI, TPA, Sun Global Desktop SOA Gateway)?	Business 2 Business (B2B) establishes a dedicated connection between an outside organization and the Citi network that remains active and available 24/7 by 365 days a year. The dedicated connection results in an "always on" connection. A direct B2B connection can only be used if SOA Gateway, Citrix/VDI, and Sun Global Desktop connectivity options are one or more of the following 1) not cost effective 2) cannot be used or 3) only application connectivity is required. Note that all B2B access requests must go through the OSTIA process identified [here]().
Please select all of the reasons that this direct connectivity is being used in lieu of a virtualized PC session:	If you must use direct B2B connection, identify the reason(s) why you are unable to use a virtualized connectivity solution. The three available options are the only possible exceptions. If none of these apply, you must use the virtualized connection solution. • Not Cost Effective • Application connectivity is required A virtualized PC session will not work (Examples of virtualized sessions include; SOA Gateway, Citrix / VDI / Third Party Access (TPA) Sun Global Desktop)
Connectivity Justification **By audit requirement it is critical that you provide sufficient details around the BUSINESS JUSTIFICATION for the connectivity you are requesting.**	All change request must have business details providing an explanation as to why the connection is required. Please provide a clear and documented benefit to Citi businesses or customers. The connectivity must be legally permissible, have ISO approval and be represented by a Citi Employee. Attempt to provide answers to all of the following questions.. What business processes and owners of these processes are being supported? What systems and or applications are used in this process? Is this a new process or a change to an existing process or service? Please make sure to include Citi SOW number(s) if applicable, any other supporting details. Note: Requests containing insufficient detail will result in delay of processing of the request or cancelation. * All Merger / Acquisitions / Divestitures must have an active Transition Services Agreement (TSA) for all requests..

Business Case

Field	Explanation / Data To Enter
ServiceNow Business CAB Approver Group/Code. Supplying the Business CAB RFC Approver Code may help reduce the number of RFC approvers required.	Please provide a ServiceNow Business CAB RFC Approver Code. Supplying the Business CAB RFC Approver Code may help reduce the number of RFC approvers required.. You can look them up here: RFC CAB Approver Codes . Please select your choice ONLY from the "ID" columnn
Do not implement before Do not implement before	Populate with a date when there is potential risk associated to the connection if it were to be implemented prior to a certain date. For example, if a contract between Citi and a Third Party indicates data transfer is not to commence before 5/1/2013, then this date should be provided here.
Requestor - (must be Citi employee/FTE): * Requestor - must be Citi Employee/FTE No Value Set Update	Enter the SOEID of the Citi FTE (full time employee) who is requesting connectivity.
Business Owner-Primary: *Business Owner - Primary No Value Set Update	Enter the SOEID of the Citi FTE (full time employee) who will be responsible for connectivity. Note: The Primary business owner will be responsible for providing connectivity details, confirmations, and completion of annual connectivity verification reviews.

Business Owner-Secondary: *Business Owner - Secondary No Value Set [Update]	Enter the SOEID of the Citi FTE (full time employee) who will be a back up or secondary resource for the connectivity. Note: The Secondary business owner will be able to providing connectivity details, confirmations, and completion of annual connectivity verification reviews.
Project Coordinator: *Project Coordinator No Value Set [Update]	Enter the SOEID of the individual who is submitting the request on behalf of the business or managing the Connectivity Project. This individual will have no ownership of the connection, but will be utilized as a resource for project and connectivity details.
ISO: *ISO [Look Up]	Enter the SOEID of the Business Information Security Officer responsible for verifying the business request requirements when needed.. If you do not know the BISO, please contact the business manager for assistance. Otherwise you may use the Locate Your BISO tool located here (http://www.citigroup.net/informationsecurity/locate_biso.htm). An ISO will no longer be notified or required to review/approve new connectivity requests or changes to connectivity requests. You should however be aware that an ISO contact will continue to be collected for every connection request record. You will receive an automated system e-mail notifying you have been selected as an ISO contact for a connection request, and provide you the opportunity to opt out if this selection was made in error. Reasons an ISO contact is required for a connectivity request record are as follows: • In the event that the External Connectivity Analyst needs to contact you about the change requested in the record. • As an escalation point for the Annual Connectivity Verification (ACV) process where the business owner has been unresponsive. • As an escalation point in the Buscrit/EMER or Temporary Approval process where the business owner has been unresponsive. Any ISO (BISO, TISO, or GISO) who supports the business can be selected.

Business Tester: *Business Tester No Value Set Update	Enter the SOEID of the business contact responsible for testing, or coordination of the testing, of the connectivity once it has been implemented. The tester will be listed on the RFC and will be required to provide confirmation of his successful testing. The tester can be the same as the Primary/Secondary owner.
Managing Director * Managing Director No Value Set Update	Use the provided search functionality to find the Managing Director who will provide their approval to proceed with the EMER/BUSCRIT request. Note: The search box is limited to Citi employees with MD or higher title.

Third Party Details

This section of the Marketplace form is used to obtain information regarding Third Party vendors. All proxy requests need to have this information populated.

Field	Explanation / Data To Enter
Who will this request for connectivity service? * Who will this request for connectivity service? (Please select) (Please select) Client, Customer, Partner Vendor, Supplier, Regulatory Agency, Government Agency Internal Users, Internal Connectivity	Select Client, Customer, Partner or vendor, supplier, partner, client, or government agency, these are all considered Third Party. If the destination is not Citi owned, then it is considered a third party
Vendor Contractual Statement of Work: Vendor Contractual Statement of Work Remaining characters: 255	Enter the Vendor contractual Statement of Work (SOW) number associated with the connectivity request. This will be used for review of the project details, connectivity tracking, and Entitlement reviews.

Please upload Vendor Documentation outlining the traffic flow and/or how the application works * Please upload Vendor Documentation outlining the traffic flow and/or how the application works. No Attachment Update	Upload Vendor Documentation outlining the traffic flow and/or how the application works
Third Party Company Name: * Third Party Name	Provide the name of the Third Party organization who will be utilizing the connectivity that requires access through the Firewall
CASP Supplier ID: * CASP Supplier ID	Enter the CASP [Citi Approved Supplier Program] Supplier number associated with the third party vendor. This information may be obtained by querying the CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp) A CASP Supplier ID must be obtained and entered before a Third Party firewall modification can be processed. If the third party has not been registered in CASP please review the process requirements in the FAQ (https://casp.ny.ssmb.com/casp/popups/file.asp?filename=FAQ.doc&ID=0)
CASP Detail ID: * CASP Detail ID	Enter the CASP [Citi Approved Supplier Program] Detail ID corresponding to the Supplier and Business relationship. This information may be obtained by querying the CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp) A CASP Detail ID must be obtained and entered before a Third Party firewall modification can be processed. If the third party has not been registered in CASP please review the process requirements in the FAQ (https://casp.ny.ssmb.com/casp/popups/file.asp?filename=FAQ.doc&ID=0)
Third Party Contact Name: * Third Party Contact Name	Enter the name of the contact person at the Third Party. This information can be obtained from the CASP Procurement Manager listed for the Third Party in CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)

Third Party Contact Type:	
* Third Party Contact Type (Please select) Relationship Manager Supplier Third Party Contact Technical Support	Select the current role of the contact at the third party.
Third Party Contact Phone: * Third Party Contact Phone	Enter the phone number of the contact person at the Third Party. This information can be obtained from the CASP Procurement Manager listed for the Third Party in CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)
Third Party Contact E-mail: * Third Party Contact E-Mail	Enter the Email Address of the contact person at the Third Party. This information can be obtained from the CASP Procurement Manager listed for the Third Party in CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)

Technical Details

This questions appearing in this section are dependent on the type of Proxy connection you are submitting and is defined by your response to question "Proxy Type" in the Business Justification section. Please refer to section headers to determine which one best correlates to your submission request.

Filter/White list

Field	Explanation / Data To Enter
Please estimate how frequently this connectivity will be used * Please estimate how frequently this connectivity will be used Biweekly (Please select) Daily Weekly Biweekly Monthly Bimonthly Quarterly Semi-Annual Annual As-needed (no set schedule, example: COB)	Select the data frequency

Indicate the type and highest classification of data being accessed with this connectivity. Data must be encrypted end to end if it is Confidential or Higher *Customer Data (Please select) (Please select) Public Internal Confidential Restricted Not Applicable *Citi Data (Please select) (Please select) Public Internal Confidential Restricted Not Applicable	Select the classification that best corresponds to the data that is being transferred. **Confidential:** Information that Citi Businesses are obligated to protect including, but not limited to information belonging to: customers, Workers, Third Parties, or Citi Businesses. Any combination of data subject to regulatory or contractual restrictions on disclosure. Information that the Business determines has the potential to provide a competitive advantage or have a significant impact on the Business if disclosed to unauthorized individuals. **Internal:** Information that is commonly shared within Citi is not intended for distribution outside Citi and is not classified as Restricted or Confidential. **Public:** Information that is freely available outside of Citi or is intended for public use by the Information Owner. **Restricted:** Information that, if disclosed to unauthorized individuals, could have a significant impact on Citi's legal or regulatory obligations or on its financial status, customers or franchise. **N/A:** No Data will be transferred.
Filter - Is Internet access required? Filter - Is Internet access required? (Please select) (Please select) Yes No	Select yes or No
Filter – Proxy Instance, Port or Proxy Setting Filter - Proxy Instance, Port or Proxy Setting Remaining characters: 255	If known, provide the port number or proxy setting to be used for the Filter/White list Proxy request. If this information is not known to you it may be left blank.

Filter – Please complete spreadsheet here and upload to request:	Download this [spreadsheet](https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/Proxy%20Filter.xlsx) (https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/Proxy%20Filter.xlsx) and populate all columns with the information pertaining to your request.
*Filter - Please complete spreadsheet here and upload this to request Update	Once completed, upload the spreadsheet to the CMP product.
Please paste your proxy setting: *Please paste your proxy setting	You can find your proxy setting by going to IE -> Tools -> Internet Options -> Connections -> LAN settings -> Configuration Address. Provided proxy settings will be used for the technical registration details.

PAC FILE

Proxy Auto-Configuration (PAC) Files are used to assist the proxy configuration. The files will contain small scripts the proxy will use to direct connectivity.

Field	**Explanation / Data To Enter**
Please estimate how frequently this connectivity will be used *Please estimate how frequently this connectivity will be used Biweekly (Please select) Daily Weekly Biweekly Monthly Bimonthly Quarterly Semi-Annual Annual As-needed (no set schedule, example: COB)	Select the data frequency

Indicate the type and highest classification of data being accessed with this connectivity. Data must be encrypted end to end if it is Confidential or Higher *Customer Data (Please select) (Please select) Public Internal Confidential Restricted Not Applicable *Citi Data (Please select) (Please select) Public Internal Confidential Restricted Not Applicable	Select the classification that best corresponds to the data that is being transferred. **Confidential:** Information that Citi Businesses are obligated to protect including, but not limited to information belonging to: customers, Workers, Third Parties, or Citi Businesses. Any combination of data subject to regulatory or contractual restrictions on disclosure. Information that the Business determines has the potential to provide a competitive advantage or have a significant impact on the Business if disclosed to unauthorized individuals. **Internal:** Information that is commonly shared within Citi is not intended for distribution outside Citi and is not classified as Restricted or Confidential. **Public:** Information that is freely available outside of Citi or is intended for public use by the Information Owner. **Restricted:** Information that, if disclosed to unauthorized individuals, could have a significant impact on Citi's legal or regulatory obligations or on its financial status, customers or franchise. **Not Applicable:** No Data will be transferred.
PAC - Is Internet access required? *PAC - Is Internet access required? (Please select) (Please select) Yes No	Select Yes Or No

PAC – Please complete spreadsheet here and upload to this request *PAC - Please complete spreadsheet here and upload this to request [Update]	Download this spreadsheet (https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/Proxy_PACFILE.xls) and populate all columns with the information pertaining to your request. Please review the sample entry for guidance. Once completed, upload the spreadsheet to the CMP product. Only requests submitted using the approved formatted spreadsheet will be accepted.
PAC – Proxy Instance, Port or Proxy Setting (If Known) PAC - Proxy Instance, Port or Proxy Setting [ ] Remaining characters: 255	If known, provide the port number or proxy setting to be used for the PAC Proxy request. If this information is not known to you it may be left blank.
Please paste your proxy setting: *Please paste your proxy setting [ ]	You can find your proxy setting by going to IE -> Tools -> Internet Options -> Connections -> LAN settings -> Configuration Address. Provided proxy settings will be used for the technical registration details.

Plug

A Plug will map an IP address and port to a specific location on the internet. Proxy Plugs should be avoided if a SOCKS proxy option is available in the client software, as it can interfere with proper security negotiations.

Field	Explanation / Data To Enter

Is the application registered in CSI? (Please select) (Please select) Yes No	Select whether the application you wish to provide connectivity to/from has already been registered in the [Citi Systems Inventory](#) If you select YES, you will need to look up the CSI application **Please select the CSI application** Look Up If the application is registered in CSI then use the search functionality to look for, and select, the appropriate registration.
Please estimate how frequently this connectivity will be used * Please estimate how frequently this connectivity will be use Biweekly (Please select) Daily Weekly Biweekly Monthly Bimonthly Quarterly Semi-Annual Annual As-needed (no set schedule, example: COB)	Select the data frequency

Indicate the type and highest classification of data being accessed with this connectivity. Data must be encrypted end to end if it is Confidential or Higher *Customer Data (Please select) (Please select) Public Internal Confidential Restricted Not Applicable	Select the classification that best corresponds to the data that is being transferred. **Confidential:** Information that Citi Businesses are obligated to protect including, but not limited to information belonging to: customers, Workers, Third Parties, or Citi Businesses. Any combination of data subject to regulatory or contractual restrictions on disclosure. Information that the Business determines has the potential to provide a competitive advantage or have a significant impact on the Business if disclosed to unauthorized individuals. **Internal:** Information that is commonly shared within Citi is not intended for distribution outside Citi and is not classified as Restricted or Confidential. **Public:** Information that is freely available outside of Citi or is intended for public use by the Information Owner. **Restricted:** Information that, if disclosed to unauthorized individuals, could have a significant impact on Citi's legal or regulatory obligations or on its financial status, customers or franchise. **Not Applicable:** No Data will be transferred
Is the data being transferred Citi owned? *Is the data being transferred Citi owned? (Please select) (Please select) Yes No	Select "yes' Or "no"
*Is the traffic encrypted? If so, How?	If the traffic has encryption enabled please explain in detail what type of encryption it is.
*Is this Plug/Socks for a Push, Pull or both a Push & Pull of Data? (Please select) (Please select) Push Pull Both	Will Citi initiate a push or pull or both a push and pull file transfer?

*Frequency of Transfer Remaining characters: 255	How often will the data be transfers via the Proxy connection? Daily, Weekly, Monthly, Bi Yearly, Yearly?
*File Size Remaining characters: 255	What is the average file size that will be transmitted per transfer?
*Is there an existing B2B connection that can be utilized in lieu of socks/plug? (Please select) (Please select) Yes No	Does Citi currently have a B2B connection with the third party that would enable the business to transfer the data without the use of a proxy? If you select, YES, you will need to provide justification.
Plug - Proxy Port (if known)	If known, provide the port to be used by the plug.
Plug – Please complete spreadsheet here and upload this to the request ***Plug - Please complete spreadsheet here and upload this to request** Update	Download this spreadsheet (https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/Proxy_PLUG.xls) and populate all columns with the information pertaining to your request. Please review the sample entry for guidance. Once completed, upload the spreadsheet to the CMP product. Only requests submitted using the approved formatted spreadsheet will be accepted.

SOCKS

A SOCKS uses an on-demand negotiation between the client application and the proxy to establish connectivity.

Field	Explanation / Data To Enter

*What version of SOCKS will be used? (Please select) (Please select) 4 4a 5	**What SOCK protocol version will be used for the sock connectivity?** **4:** Base level protocol **4A:** extends the SOCKS4 protocol to allow a client to specify a destination domain name rather than an IP address **5:** offers more choices for authentication, and adds support for IPv6 and UDP
*Is the application registered in CSI? (Please select) (Please select) Yes No	**Citi Systems Inventory** If you select Yes, please search for the CSI ID **Please select the CSI application** Look Up If the application is registered in CSI then use the search functionality to look for, and select, the appropriate registration
Please estimate how frequently this connectivity will be used *Please estimate how frequently this connectivity will be used Biweekly (Please select) Daily Weekly Biweekly Monthly Bimonthly Quarterly Semi-Annual Annual As-needed (no set schedule, example: COB)	Select the data frequency
Is the data being transferred Citi owned? *Is the data being transferred Citi owned? (Please select) (Please select) Yes No	Select "yes" or 'No"
*Is the traffic encrypted? If so, How?	If the traffic has encryption enabled please explain in detail what type of encryption it is.

*Is this Plug/Socks for a Push, Pull or both a Push & Pull of Data? (Please select) (Please select) Push Pull Both	Will Citi initiate a push or pull or both a push and pull file transfer?
*Frequency of Transfer [ ] *Remaining characters: 255*	How often will the data be transfers via the Proxy connection? Daily, Weekly, Monthly, Bi Yearly, Yearly
*File Size [	] *Remaining characters: 255*	What is the average file size that will be transmitted per transfer?
*Is there an existing B2B connection that can be utilized in lieu of socks/plug? (Please select) (Please select) Yes No	Does Citi currently have a B2B connection with the third party that would enable the business to transfer the data without the use of a proxy?
SOCKS Rule (if known) [ ] *Remaining characters: 255*	Enter the SOCKs rule
*Click here to download the Proxy-Socks connectivity template. Upload the completed template below finalized. No Attachment [Update]	Download this spreadsheet (https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/SOCKS%20Request.xls) and populate all columns with the information pertaining to your request. Please review the sample entry for guidance. Once completed, upload the spreadsheet to the CMP product. Only requests submitted using the approved formatted spreadsheet will be accepted.

New Proxy Instance

A New Proxy Instance should be part of the initial project of establishing connectivity into the Citi GRN. A new instance should include a URL list to create a Filter/Whitelist, and a Pac file; depending on the user needs

Field	Explanation / Data To Enter
Please estimate how frequently this connectivity will be used * Please estimate how frequently this connectivity will be used Biweekly (Please select) Daily Weekly Biweekly Monthly Bimonthly Quarterly Semi-Annual Annual As-needed (no set schedule, example: COB)	Select the data frequency

	Select the classification that best corresponds to the data that is being transferred.
Indicate the type and highest classification of data being accessed with this connectivity. Data must be encrypted end to end if it is Confidential or Higher *Customer Data (Please select) (Please select) Public Internal Confidential Restricted Not Applicable *Citi Data (Please select) (Please select) Public Internal Confidential Restricted Not Applicable	**Confidential:** Information that Citi Businesses are obligated to protect including, but not limited to information belonging to: customers, Workers, Third Parties, or Citi Businesses. Any combination of data subject to regulatory or contractual restrictions on disclosure. Information that the Business determines has the potential to provide a competitive advantage or have a significant impact on the Business if disclosed to unauthorized individuals. **Internal:** Information that is commonly shared within Citi is not intended for distribution outside Citi and is not classified as Restricted or Confidential. **Public:** Information that is freely available outside of Citi or is intended for public use by the Information Owner. **Restricted:** Information that, if disclosed to unauthorized individuals, could have a significant impact on Citi's legal or regulatory obligations or on its financial status, customers or franchise. **Not Applicable:** No Data will be transferred.
New Proxy Instance – Please complete spreadsheet here and upload this to the request *New Proxy Instance - Please complete spreadsheet here and upload this to request Update	Download and populate the spreadsheet (https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/ New%20Instance%20.xlsx), only requests submitted using the approved formatted spreadsheet will be accepted. The spreadsheet provides examples for assistance

New Proxy Instance – Proxy Instance, Port or Proxy Setting (If Known) New Proxy Instance - Proxy Instance, Port or Proxy Setting	Please provide the port number or proxy setting to be used for the new Proxy instance. If this information is not known to you it may be left blank.
New Proxy Instance – Intended Purpose *New Proxy Instance - Intended Purpose |	The intended purpose must be specific and detailed. A lack of clarity on the purpose can delay connectivity requests as the deployment team will need to manually obtain the details.
New Proxy Instance – Is internet access via Citi proxy required? *New Proxy Instance - Is Internet access via Citi proxy required? (Please select) (Please select) Yes No	Does the user require access to URLs outside of the Citi Network; these URLs would be considered part of the external Internet.
New Proxy Instance – Number of additional PAC files required? * New Proxy Instance - Number of additional PAC files required? (Please select) N/A 1 2 3 4 5	Each individual PAC file will contain scripts that the proxy will utilize for routing the connectivity requests. Each specific routing requirement will need a separate PAC file.
Please paste your proxy setting *Please paste your proxy setting	You can find your proxy setting by going to IE -> Tools -> Internet Options -> Connections -> LAN settings -> Configuration Address. Provided proxy settings will be used for the technical registration details.

Free URL

Field	Explanation / Data To Enter
Please estimate how frequently this connectivity will be used *Please estimate how frequently this connectivity will be used Biweekly (Please select) Daily Weekly Biweekly Monthly Bimonthly Quarterly Semi-Annual Annual As-needed (no set schedule, example: COB)	Select the data frequency
Indicate the type and highest classification of data being accessed with this connectivity. Data must be encrypted end to end if it is Confidential or Higher *Customer Data (Please select) (Please select) Public Internal Confidential Restricted Not Applicable *Citi Data (Please select) (Please select) Public Internal Confidential Restricted Not Applicable	Select the classification that best corresponds to the data that is being transferred. **Confidential:** Information that Citi Businesses are obligated to protect including, but not limited to information belonging to: customers, Workers, Third Parties, or Citi Businesses. Any combination of data subject to regulatory or contractual restrictions on disclosure. Information that the Business determines has the potential to provide a competitive advantage or have a significant impact on the Business if disclosed to unauthorized individuals. **Internal:** Information that is commonly shared within Citi is not intended for distribution outside Citi and is not classified as Restricted or Confidential. **Public:** Information that is freely available outside of Citi or is intended for public use by the Information Owner. **Restricted:** Information that, if disclosed to unauthorized individuals, could have a significant impact on Citi's legal or regulatory obligations or on its financial status, customers or franchise. **Not Applicable:** No Data will be transferred.

FreeUrl – Please complete spreadsheet here and upload to this request	Download this spreadsheet (https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/ Free%20URL%20list.xlsx) and populate all columns with the information pertaining to your request. Please review the sample entry for guidance.
*PAC - Please complete spreadsheet here and upload this to request [Update]	Once completed, upload the spreadsheet to the CMP product. Only requests submitted using the approved formatted spreadsheet will be accepted.
Please paste your proxy setting: *Please paste your proxy setting	You can find your proxy setting by going to IE -> Tools -> Internet Options -> Connections -> LAN settings -> Configuration Address. Provided proxy settings will be used for the technical registration details.

Priority Questions

This section of the Marketplace form is required when the connection urgency has been entered as either *Business Critical* or *Emergency* under section *Project Details*. The justification is required for submission of why the request cannot be entered as *BAU (Business as Usual*.

The questions will only need to be populated if the request is not BAU (Business as Usual) as per your selection in the *Project Details* section.

Field	Explanation / Data To Enter
VT (Sev 1-2), ServiceNow or EMS Number *VT (SEV 1-2), ServiceNow or EMS Number	*#Only required for EMERs#* All Firewall submissions with *Request Urgency* of *Emergency* require an associated Virtual Ticket ServiceNow ID or EMS Number. Emergency requests without a valid number will not be processed.

Provide the name/SOE ID of the approving Senior Managing Director ***Provide the name/SOE id of the approving Senior Managing Director** No Value Set Update	Use the provided search functionality to find the Managing Director who will provide their approval to proceed with the EMER/BUSCRIT request. Note: The search box is limited to Citi employees with MD or higher title.
Which business is requesting the change if different from the group raising the RFC? ***Which business is requesting the change if different from the group raising the RFC?**	Populate the business following Global Directory formatting standards.
Which department is the owner of this process? ***Which department is the owner of this process?**	Populate the department following Global Directory formatting standards.
Describe the business impact if the change does not occur out of cycle. ***Describe the impact to the Business if this change does not occur out of cycle.**	Explain, in detail, what negative impact would affect the business and/or Citi as a whole if the firewall modification is not made in an expedited fashion. Provide as much detail as possible, including contract deadlines, financial loss amounts, or penalties. This information will be reviewed, and confirmed, to determine whether your request does, in fact, require expedited handling.
Does any additional business testing need to take place for this unplanned change? ***Does any additional Business testing need to take place for this unplanned change? (Provide details)** Remaining characters: 255	Please note if your business requires testing beyond the normal implementation verification step that will be completed after the firewall change has occurred. Additional business testing can include verification that the destination and source application are compatible and verification that the two applications are running as expected pre-change.

What process failed that prevented this change from being able to follow the normal change cycle?. *What process failed that prevented this change request from being able to follow the standard change cycle?	Explain, in detail, why this request was not submitted to the External Connectivity Management team with sufficient time to undergo the normal change cycle. This information will be reviewed, and confirmed, to determine whether your request does, in fact, require expedited handling.
Are there any other changes scheduled during the same time frame for the same or related environment ? *What other changes, if any, are scheduled during the same time frame for the same or a related environment that may clash with this request? (Provide details)	Provide details on known changes that will be occurring during the time frame you are requesting a firewall change be made. Any changes potentially affecting the source or destination networking environments should be noted.

Additional Information

Please assist the processing team by answering the following optional questions to help in expediting your request.

Field	Explanation / Data To Enter
Other Documentation	Use this option to provide any documentation you would like the reviewer to take into consideration
Comments **Comments**	Use this space to enter any additional information you would like the reviewer to take into consideration

What to Expect Next

Once the CMP request has been completed, the request will be routed to the External Connectivity Management team and a specialist will be assigned to support the request. The External Connectivity Specialist will review the request details and reach out to the submitter for clarification on any incorrect/outstanding items before transferring the request into the Citi Connectivity Registry. If at any time the External Connectivity team reaches out to the business for additional information and no response is received within 14 days, the CMP may be considered closed.

Certain requests will be classified as high risk or non-standard; high risk requests are defined as those that require access through a source, destination and port combination that contain known vulnerabilities. These combinations are detailed on the protected excel file located here https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/High%20Risk.xlsx

In order to compensate for the vulnerabilities created by these high risk requests the business will be required to provide information/controls above and beyond that of a regular request.

Type	Action	SLO*
EMER BUSCRIT	Managing Director Approval A senior manager, at the Managing Director Level or higher, must approve all requests submitted with urgency of Emergency or Business Critical. The MD approval will be done through resolve it after receipt of an automated email notification generated upon submission of the Citi Market Place request.	Business Dependent. *Historical Median:* 0.2 days
High Risk	OSTIA [Operating System Trust or Interactive Access] Questionnaire OSTIA Questionnaire is required for connectivity requests that a) allows the client machine to directly access the host machine on the Citi internal network at the operating system level or b) allows the target user to have command shell access to the operating system or c) uses any port that is used for non-default services. If the request constitutes as an OSTIA item, you will be required to provide additional information to the ECM [External Connectivity Management] team via email. Click on the header of this section to obtain details on what will be required.	Business Dependent.
High Risk Non Standard	Global Information Security (GIS) Review Once approved by the business and ECM, the request is routed to GIS for review against security standards and OSTIA guidelines. If the request complies with all requirements, it is sent for implementation. If there are any issues, or the request is deemed a high risk, the request is schedule for Working Group review.	1 day
Requests marked during GIS	Third Party Working Group Approval All requests marked for review by GIS Review, require a higher level Third Party Working Group Approval. The Third Party Access Solutions	7 days *Historical Median:*

review	Working Group operates under the direction of the Information Security Risk Operating Committee (ISROC) to review connectivity requests that traverse the Citi perimeter. requests TPASWG review happens every Tuesday at 9am ET. Cutoff for each week's review is Monday 12 noon ET for ISO approval completion. Click on the header of this section to obtain additional information on the approval process.	1.3 days
All	Connectivity Verification Upon approval of the RFC request, the Primary/Secondary Business Owner [as selected on the original CMP request] will receive an email requesting they prepare to verify the connection was successfully implemented. Requestor should notify the ECM team prior to the day of the change if there are any special testing requirements, like joining a particular audio bridge or providing support during long-duration testing/check out periods. Requestor should also notify ECM if they do not plan on testing, and confirm that they accept the risk of the change not work as planned after the change green zone has ended. If the connection works as planned the requestor should notify ECM that the change was tested and that they are satisfied that the connectivity is functioning correctly. If there are implementation errors identified during the green zone, the deployment team will make the necessary updates and ensure the connection is functioning as planned.	Business Dependent.
All	Annual Connectivity Verification 365 days after the implementation the Primary/Secondary Business Owner [as selected on the original CMP request] will receive an email requesting they complete the Annual Connectivity Verification. You have 90 days to complete the ACV. If the ACV is not completed it will be reported on the monthly report to Senior Management. Click on the header of this section to obtain additional information.	Business Dependent 90 Day Max
All	Notifications Business users assigned to the request as Submitter, Information Security Officer, Business Manager, Project Coordinator, and Technical coordinator will receive email notifications when an action is required. Please ensure that you pay special attention to any emails coming from ***OTRM US CCR** or containing **"CCR Notification"** on the subject line. For additional details on the notifications please review the Notifications section in the appendix.	N/A

IP Registration
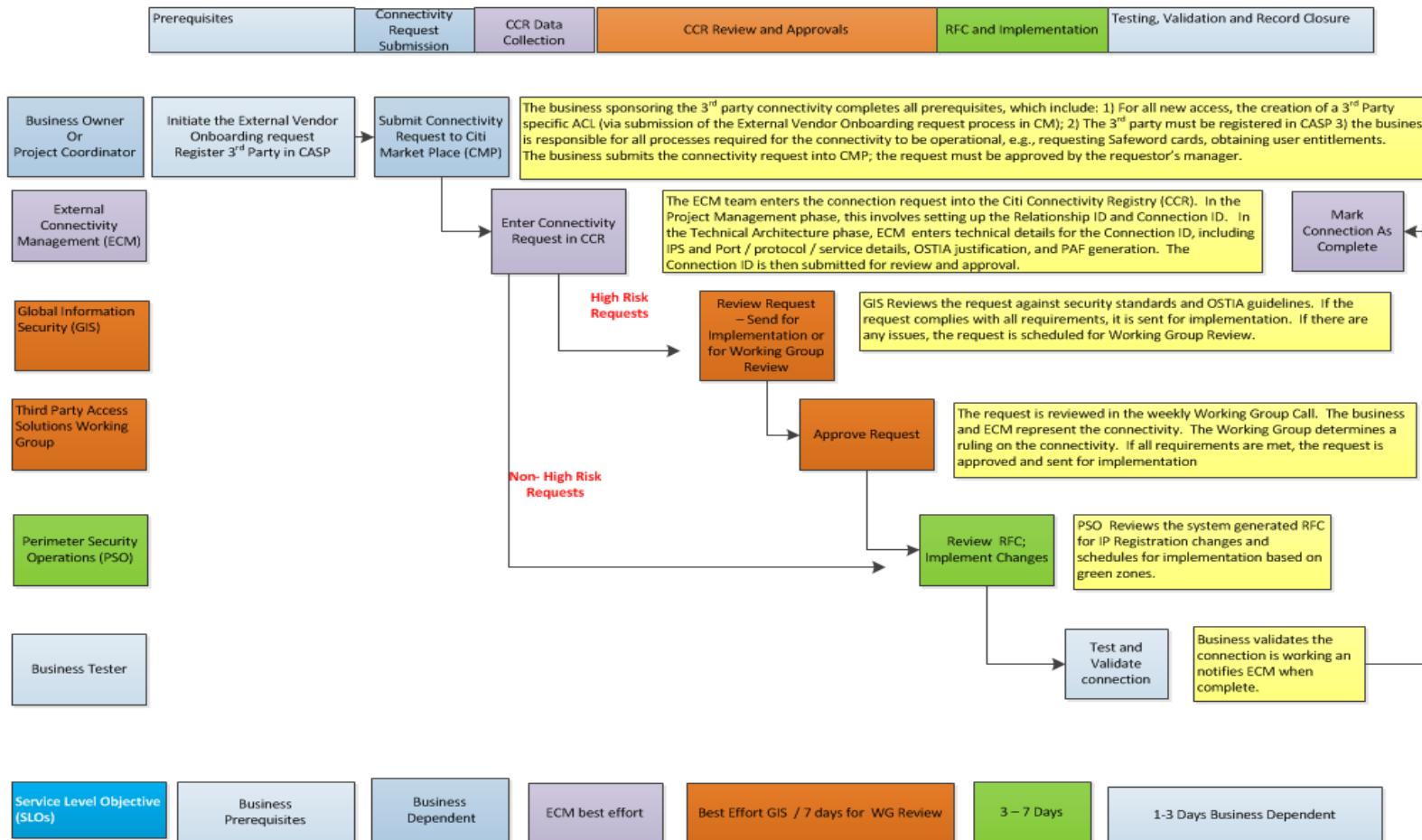
Introduction to IP Registration Requests

IP registrations enable connectivity that allows remote access to specific devices on the Citi Network via a non-fixed Internet location. Each request is either for Citi Employees or specific Third Parties. Citi Employees belong to a single Access Control List (ACL) and each vendor belongs to their specific ACL. The Access Control List determines what resources the connecting party may access within the Citi network.
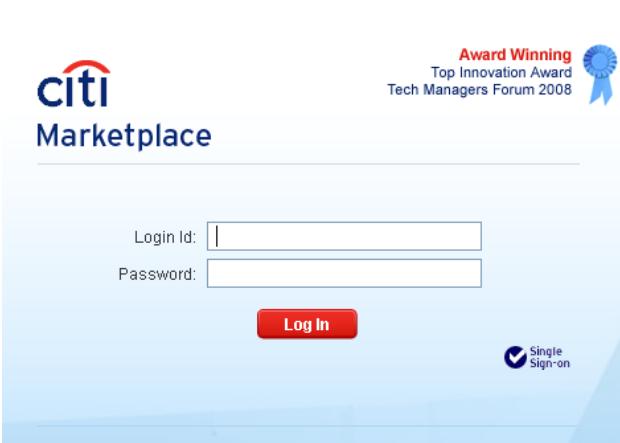
The connectivity between the remote party and the Citi device will utilize the Citi Cisco AnyConnect Secure Mobility Client via the Internet. This client works by creating a secure, encrypted tunnel between the end user and the Citi destination. End users will authenticate to Cisco AnyConnect using a Citi provided Safeword Card that issues temporary passwords.

IP Registration Workflow

Prerequisites	Connectivity Request Submission	CCR Data Collection	CCR Review and Approvals	RFC and Implementation	Testing, Validation and Record Closure

Business Owner Or Project Coordinator → Initiate the External Vendor Onboarding request Register 3rd Party in CASP → Submit Connectivity Request to Citi Market Place (CMP)

The business sponsoring the 3rd party connectivity completes all prerequisites, which include: 1) For all new access, the creation of a 3rd Party specific ACL (via submission of the External Vendor Onboarding request process in CM); 2) The 3rd party must be registered in CASP 3) the business is responsible for all processes required for the connectivity to be operational, e.g., requesting Safeword cards, obtaining user entitlements. The business submits the connectivity request into CMP; the request must be approved by the requestor's manager.

External Connectivity Management (ECM) → Enter Connectivity Request in CCR

The ECM team enters the connection request into the Citi Connectivity Registry (CCR). In the Project Management phase, this involves setting up the Relationship ID and Connection ID. In the Technical Architecture phase, ECM enters technical details for the Connection ID, including IPS and Port / protocol / service details, OSTIA justification, and PAF generation. The Connection ID is then submitted for review and approval.

Mark Connection As Complete

Global Information Security (GIS)

High Risk Requests → Review Request – Send for Implementation or for Working Group Review

GIS Reviews the request against security standards and OSTIA guidelines. If the request complies with all requirements, it is sent for implementation. If there are any issues, the request is scheduled for Working Group Review.

Third Party Access Solutions Working Group

Approve Request

The request is reviewed in the weekly Working Group Call. The business and ECM represent the connectivity. The Working Group determines a ruling on the connectivity. If all requirements are met, the request is approved and sent for implementation

Non- High Risk Requests

Perimeter Security Operations (PSO)

Review RFC; Implement Changes

PSO Reviews the system generated RFC for IP Registration changes and schedules for implementation based on green zones.

Business Tester

Test and Validate connection

Business validates the connection is working an notifies ECM when complete.

Service Level Objective (SLOs)	Business Prerequisites	Business Dependent	ECM best effort	Best Effort GIS / 7 days for WG Review	3 – 7 Days	1-3 Days Business Dependent

Submitting IP Registration Marketplace Order

The Citi Market Place form required to initiate the request can be accessed by following the below steps

	Log into Citi Marketplace(https://cmp.nj.ssmb.com/marketplace/control/main) using your Single Sign On (SSO) ID.
All Categories ▼ CCR	Search for *CCR* at the top right hand of the screen
Citi Connectivity Registry Request	Select the Citi Connectivity Registry Request form

Alternatively, you may access the form directly via this link
(https://cmp.nj.ssmb.com/marketplace/control/product/~productId=31622_377493_GLOBAL#)

Request Type

The CMP form will allow you to request a brand new connectivity or to modify an existing one through a technical update to a Firewall Request. The questionnaire section for both request types require identical information be provided with only a slight exception. A technical update will request the existing CCR ID be provided, so that the specialist assigned can link the modification with the existing ID, while a New Connection does not require this information.

Field	Explanation / Data To Enter
Request Type:	
Type of Connectivity Involved:	
Is the connectivity part of an ongoing Merger, Acquisition & Divestiture effort?	

Request Urgency *Request Urgency (Please select) (Please select) BAU Business Critical Emergency	The urgency of your request is determined by the required implementation date and the potential impacts to Citi were the request not implemented. *Note that requests should not be classified as higher than BAU unless there is a justifiable business reason for doing so. **BAU:** Business As usual – Request will follow normal business SLO for implementation, typically 5 to 10 business days. **BUSCRIT:** Business Critical - Request is classified as critical, rush implementation. BUSCRIT requests require answering business critical questions and Managing Director approval. BUSCRIT SLO 3 to 5 business days. **EMER:** Emergency - Requests are classified as an emergency due to a break/fix of a production failure. EMERs require a ticket in ServiceNow, CT, or EMS, an emergency justification and Managing Director approval. **Please Note: Business Critical requests require Managing Director approval. EMERs require MD Approval and an EMS ticket number.)**
Project Sector: * Project Sector (Please select) (Please select) Corporate Center CTI GCB ICG	Select the Sector of the business who will own the connectivity.
Project Region: * Project Region (Please select) (Please select) ASPAC EMEA JAPAN LATAM North America	Select the region where the Business resides and the majority of the business activity will reside.

Connectivity Justification	All Firewall change request must have business details providing an explanation as to why the connection is required. Please provide a clear and documented benefit to Citi businesses or customers. The connectivity must be legally permissible, have ISO approval and be represented by a Citi Employee.
By audit requirement it is critical that you provide sufficient details around the BUSINESS JUSTIFICATION for the connectivity you are requesting.	Attempt to provide answers to all of the following questions.. What business processes and owners of these processes are being supported? What systems and or applications are used in this process? Is this a new process or a change to an existing process or service? Please make sure to include Citi SOW number(s) if applicable, any other supporting details. Note: Requests containing insufficient detail will result in delay of processing of the request or cancelation. * All Merger / Acquisitions / Divestitures must have an active Transition Services Agreement (TSA) for all requests..

Business Case

Field	Explanation / Data To Enter
ServiceNow Business CAB Approver Group/Code. Supplying the Business CAB Approver Code may help reduce the number of approvers required.	Please provide a ServiceNow Business CAB RFC Approver Code. Supplying the Business CAB RFC Approver Code may help reduce the number of RFC approvers required.. You can look them up here: RFC CAB Approver Codes . Please select your choice ONLY from the "ID" columnn
Do not implement before Do not implement before [ ]	Populate with a date when there is potential risk associated to the connection if it were to be implemented prior to a certain date. For example, if a contract between Citi and a Third Party indicates data transfer is not to commence before 5/1/2013, then this date should be provided here.

	Select the region where the Business resides and the majority of the business activity will reside.
Requestor - (must be Citi employee/FTE): * Requestor - must be Citi Employee/FTE No Value Set **Update**	Enter the SOEID of the Citi FTE (full time employee) who is requesting connectivity.
Business Owner-Primary: * Business Owner - Primary No Value Set Update	Enter the SOEID of the Citi FTE (full time employee) who will be responsible for connectivity. Note: The Primary business owner will be responsible for providing connectivity details, confirmations, and completion of annual connectivity verification reviews.
Business Owner-Secondary: * Business Owner - Secondary No Value Set Update	Enter the SOEID of the Citi FTE (full time employee) who will be a back up or secondary resource for the connectivity. Note: The Secondary business owner will be able to providing connectivity details, confirmations, and completion of annual connectivity verification reviews.
Project Coordinator: * Project Coordinator No Value Set Update	Enter the SOEID of the individual who is submitting the request on behalf of the business or managing the Connectivity Project. This individual will have no ownership of the connection, but will be utilized as a resource for project and connectivity details.

ISO: *ISO Look Up	Enter the SOEID of the Business Information Security Officer responsible for verifying the business request requirements when needed.. If you do not know the BISO, please contact the business manager for assistance. Otherwise you may use the Locate Your BISO tool located here (http://www.citigroup.net/informationsecurity/locate_biso.htm). An ISO will no longer be notified or required to review/approve new connectivity requests or changes to connectivity requests. You should however be aware that an ISO contact will continue to be collected for every connection request record. You will receive an automated system e-mail notifying you have been selected as an ISO contact for a connection request, and provide you the opportunity to opt out if this selection was made in error. Reasons an ISO contact is required for a connectivity request record are as follows: - In the event that the External Connectivity Analyst needs to contact you about the change requested in the record. - As an escalation point for the Annual Connectivity Verification (ACV) process where the business owner has been unresponsive. - As an escalation point in the Buscrit/EMER or Temporary Approval process where the business owner has been unresponsive. Any ISO (BISO, TISO, or GISO) who supports the business can be selected.
Business Tester: *Business Tester No Value Set Update	Enter the SOEID of the business contact responsible for testing, or coordination of the testing, of the connectivity once it has been implemented. The tester will be listed on the RFC and will be required to provide confirmation of his successful testing. The tester can be the same as the Primary/Secondary owner.

Third Party Details

This section of the Marketplace form is used to obtain information regarding Third Party vendors. The questions will only need to be populated if the response to the first item "Does this request involve a Third Party" is yes.

Field	Explanation / Data To Enter
Who will this request for connectivity service? *Who will this request for connectivity service? (Please select) (Please select) Client, Customer, Partner Vendor, Supplier, Regulatory Agency, Government Agency Internal Users, Internal Connectivity	Select Client, Customer, Partner or vendor, supplier, partner, client, or government agency, these are all considered Third Party. If the destination is not Citi owned, then it is considered a third party.
Vendor Contractual Statement of Work Vendor Contractual Statement of Work Remaining characters: 255	Please provide Statement of Work Tracking ID wherever contract exists to support the connectivity Request.
Third Party Company Name: *Third Party Name	Provide the name of the Third Party organization who will be utilizing the connectivity that requires access through the Firewall

CASP Supplier ID: *CASP Supplier ID	Enter the CASP [Citi Approved Supplier Program] Supplier number associated with the third party vendor. This information may be obtained by querying the CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp) A CASP Supplier ID must be obtained and entered before a Third Party firewall modification can be processed. If the third party has not been registered in CASP please review the process requirements in the FAQ (https://casp.ny.ssmb.com/casp/popups/file.asp?filename=FAQ.doc&ID=0)
CASP Detail ID: *CASP Detail ID	Enter the CASP [Citi Approved Supplier Program] Detail ID corresponding to the Supplier and Business relationship. This information may be obtained by querying the CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp) A CASP Detail ID must be obtained and entered before a Third Party firewall modification can be processed. If the third party has not been registered in CASP please review the process requirements in the FAQ (https://casp.ny.ssmb.com/casp/popups/file.asp?filename=FAQ.doc&ID=0)
Third Party Contact Name: * Third Party Contact Name	Enter the name of the contact person at the Third Party. This information can be obtained from the CASP Procurement Manager listed for the Third Party in CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)
Third Party Contact Type: * Third Party Contact Type (Please select) Relationship Manager Supplier Third Party Contact Technical Support	Select the current role of the contact at the third party.
Third Party Contact Phone: * Third Party Contact Phone	Enter the phone number of the contact person at the Third Party. This information can be obtained from the CASP Procurement Manager listed for the Third Party in CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)
Third Party Contact E-mail: * Third Party Contact E-Mail	Enter the Email Address of the contact person at the Third Party. This information can be obtained from the CASP Procurement Manager listed for the Third Party in CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)

Technical Details

You will be required to upload an excel file with the details of your connection request.

- Download and populate the form located here
  (https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/Bulk%20Upload.xls)
- Upload the document into the CMP form using the appropriate Update section

Please estimate how frequently this connectivity will be used * Please estimate how frequently this connectivity will be used Biweekly (Please select) Daily Weekly Biweekly Monthly Bimonthly Quarterly Semi-Annual Annual As-needed (no set schedule, example: COB)	Select the data frequency

| **Indicate the type and highest classification of data being accessed with this connectivity. Data must be encrypted end to end if it is Confidential or Higher** | Select the classification that best corresponds to the data that is being transferred.

Confidential:
Information that Citi Businesses are obligated to protect including, but not limited to information belonging to: customers, Workers, Third Parties, or Citi Businesses. Any combination of data subject to regulatory or contractual restrictions on disclosure. Information that the Business determines has the potential to provide a competitive advantage or have a significant impact on the Business if disclosed to unauthorized individuals.
Internal:
Information that is commonly shared within Citi is not intended for distribution outside Citi and is not classified as Restricted or Confidential.
Public:
Information that is freely available outside of Citi or is intended for public use by the Information Owner.
Restricted:
Information that, if disclosed to unauthorized individuals, could have a significant impact on Citi's legal or regulatory obligations or on its financial status, customers or franchise.
N/A:
No Data will be transferred. |

For guidance on populating the form please review the comments added to the header column of the file.

Priority Questions

This section of the Marketplace form is required when the connection urgency has been entered as either *Business Critical* or *Emergency* under section *Project Details*. The justification is required for submission of why the request cannot be entered as *BAU (Business as Usual*.

Field	Explanation / Data To Enter
VT (Sev 1-2), ServiceNow or EMS Number *VT (SEV 1-2), ServiceNow or EMS Number	*#Only required for EMER requests#* All submissions with *Request Urgency* of *Emergency* require an associated Virtual Ticket ServiceNow ID or EMS Number. Emergency requests without a valid number will not be processed.
Provide the name/SOE ID of the approving Senior Manager	Use the search functionality to look for a Managing Director level approver for the EMER or Business Critical request.
Which business is requesting the change if different from the group raising the RFC? *Which business is requesting the change if different from the group raising the RFC?	Populate the business following Global Directory formatting standards.
Which department is the owner of this process? *Which department is the owner of this process?	Populate the department following Global Directory formatting standards.

Describe the business impact if the change does not occur out of cycle. *Describe the impact to the Business if this change does not occur out of cycle. |	Explain, in detail, what negative impact would affect the business and/or Citi as a whole if the modification is not made in an expatiated fashion. Provide as much detail as possible, including contract deadlines, financial loss amounts, or penalties. This information will be reviewed, and confirmed, to determine whether your request does, in fact, require expatiated handling.
Does any additional business testing need to take place for this unplanned change? *Does any additional Business testing need to take place for this unplanned change? (Provide details) Remaining characters: 255	Please note if your business requires testing beyond the normal implementation verification step that will be completed after the change has occurred. Additional business testing can include verification that the destination and source application are compatible and verification that the two applications are running as expected pre-change.
What process failed that prevented this change from being able to follow the normal change cycle?. *What process failed that prevented this change request from being able to follow the standard change cycle?	Explain, in detail, why this request was not submitted to the External Connectivity Management team with sufficient time to undergo the normal change cycle. This information will be reviewed, and confirmed, to determine whether your request does, in fact, require expatiated handling.
Are there any other changes scheduled during the same time frame for the same or related environment ? *Are there any other changes scheduled during the same time frame for the same or related environment ? Yes (Please select) Yes No *Please explain in detail what other changes are occuring.	Provide details on known changes that will be occurring during the time frame you are requesting a change be made. Any changes potentially affecting the source or destination networking environments should be noted.

Additional Information

Please assist the processing team by answering the following optional questions to help in expediting your request.

Field	Explanation / Data To Enter
Other Documentation	Use this option to provide any documentation you would like the reviewer to take into consideration
Comments **Comments**	Use this space to enter any additional information you would like the reviewer to take into consideration

What to Expect Next

Once the CMP request has been completed, the request will be routed to the External Connectivity Management team and a specialist will be assigned to support the request. The External Connectivity Specialist will review the request details and reach out to the submitter for clarification on any incorrect/outstanding items before transferring the request into the Citi Connectivity Registry. If at any time the External Connectivity team reaches out to the business for additional information and no response is received within 14 days, the CMP may be considered closed.

Certain requests will be classified as high risk or non-standard. High risk requests are defined as those that require *new connectivity* through a source, destination and port combination that contain known vulnerabilities. These combinations are detailed on the protected excel file located here https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/High%20Risk.xlsx

In order to compensate for the vulnerabilities created by these high risk requests the business will be required to provide information/controls above and beyond that of a regular request.

Request Type	Action	SLA*
EMER BUSCRIT	**Managing Director Approval** A senior manager, at the Managing Director Level or higher, must approve all requests submitted with urgency of Emergency or Business Critical. The MD approval will be done through resolve it after receipt of an automated email notification generated upon submission of the Citi Market Place request.	Business Dependent. *Historical Median:* 0.2 days
High Risk	OSTIA [Operating System Trust or Interactive Access] Questionnaire OSTIA Questionnaire is required for connectivity requests that a) allows the client machine to directly access the host machine on the Citi internal network at the operating system level or b) allows the target user to have command shell access to the operating system or c) uses any port that is used for non-default services. If the request constitutes as an OSTIA item, you will be required to provide additional information to the ECM [External Connectivity Management] team via email. Click on the header of this section to obtain details on what will be required.	Business Dependent.
High Risk Non Standard	**Global Information Security (GIS) Review** Once approved by the business and ECM, the request is routed to GIS for review against security standards and OSTIA guidelines. If the request complies with all requirements, it is sent for implementation. If there are any issues, or the request is deemed a high risk, the request is schedule for Working Group review.	1 day

|		
Requests marked during GIS review	**Third Party Working Group Approval** All requests marked for review by GIS Review, require a higher level Third Party Working Group Approval. The Third Party Access Solutions Working Group operates under the direction of the Information Security Risk Operating Committee (ISROC) to review connectivity requests that traverse the Citi perimeter. TPASWG review occurs every Tuesday at 9am ET. The ISO review must be completed and submitted in CCR prior to 12:00 noon ET for the Monday before the Tuesday meeting in order for the request to be added to the agenda of the Working Group meeting.	7 days *Historical Median*: 1.3 days
All	Annual Connectivity Verification 365 days after the Implementation the Primary/Secondary Business Owner [as selected on the original CMP request] will receive an email requesting they complete the Annual Connectivity Verification. You have 90 days to complete the ACV. If the ACV is not completed it will be reported on the monthly report to Senior Management. Click on the header of this section to obtain additional information.	Business Dependent 90 Day Max
All	Notifications Business users assigned to the request as Submitter, Information Security Officer, Business Manager, Project Coordinator, and Technical coordinator will receive email notifications when an action is required. Please ensure that you pay special attention to any emails coming from ***OTRM US CCR** or containing **"CCR Notification"** on the subject line. For additional details on the notifications please review the Notifications section in the appendix.	N/A

Third Party Access APP Sense

Introduction to App Sense Requests

AppSense is an O&T Risk Management program that contains the ability of third party users to disrupt the entire Citi network, either maliciously or accidentally, and to ensure their compliance with Citi information security standards. All third parties accessing the Citi networking via the Third Party Architecture (TPA) virtualized environment are given a default AppSense user profile that specifies the network applications and/or ports the user is permitted to access. If the business requires an exception, that allows a third party to perform or access a blacklisted action/application, then an AppSense request must be submitted.

An example of an AppSense request is a third party developer needing to utilize ssh (tcp/22) from their TPA device to a server in one of the Citi DMZs. This type of activity is blacklisted by AppSense, and an Appsense request would need to be submitted to allow the connectivity between the TPA session for this user and the servers in the DMZ, as well as the the right to use tcp/22 from the TPA to the DMZ server.
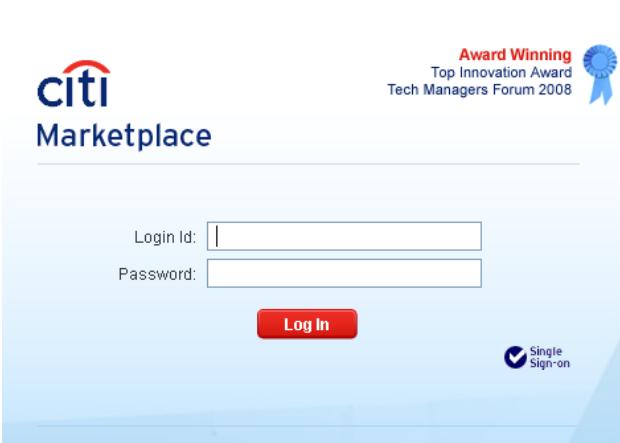
To view the complete list of blacklisted applications and protocols/ports please review the Appsense Default Blacklist (http://www.citigroup.net/informationsecurity/data/tpaswg/QRC_AppsenseDefaultBlacklist.pdf) documentation.

AppSense Workflow

Prerequisites	Connectivity Request Submission	CCR Data Collection	CCR Review and Approvals	RFC and Implementation	Testing, Validation and Record Closure

Business Owner Or Project Coordinator → Completed the TPA Connectivity Request Process → Submit Connectivity Request to Citi Market Place (CMP)

The business sponsoring the 3rd party connectivity completes all prerequisites, which include: 1) Engaging the SBC Platform team for building the Virtual Desktops; 2) Submission of firewall and proxy CM requests; 3) The business is responsible for all processes required for the connectivity to be operational, e.g., requesting Safeword Cards, obtaining user entitlements.
The business submits the connectivity request into CMP, the request must be approved by the requestor's manager.

External Connectivity Management (ECM) CCR Helpdesk → Enter Connectivity Request in CCR

The ECM CCR Helpdesk team enters the connection request into the Citi Connectivity Registry (CCR). In the Project Management phase, this involves setting up the Relationship ID and Connection ID. In the Technical Architecture phase, ECM enters technical details for the Connection ID, including IPs and Port / protocol / service details, OSTIA justification, and AAF generation. The Connection ID is then submitted for review and approval.

Mark Connection As Complete

Business Manager → Business Approval in CCR

The Business Manager or Business Owner sponsoring the connectivity, reviews and approves the connectivity request for submission as validation of business requirement

Global Information Security (GIS) → Review Request – Send for Implementation or for Working Group Review

GIS Reviews the request against security standards and OSTIA guidelines. If the request complies with all requirements, it is sent for implementation. If there are any issues, the request is scheduled for Working Group Review.

Third Party Access Solutions Working Group → Approve Request

The request is reviewed in the weekly Working Group Call. The business and ECM represent the connectivity. The Working Group determines a ruling on the connectivity. If all requirements are met, the request is approved and sent for implementation

AppSense Management Team → Implement Changes

Appsense Implementer reviews the request, schedules update for implementation based on configuration and user entitlements.

Business Tester → Test and Validate connection

Business validates the connection is working an notifies ECM CCR Helpdesk when complete.

Service Level Objective (SLOs)	Business Prerequisites	Business Dependent	ECM CCR Helpdesk best effort	Business Dependent	Best Effort GIS / 7 days for WG Review	AppSense Best Effort	1-3 Days Business Dependent

Submitting AppSense Marketplace Order

The Citi Market Place form required to initiate the request can be accessed by following the below steps

	Log into Citi Marketplace(https://cmp.nj.ssmb.com/marketplace/control/main) using your Single Sign On (SSO) ID.
	Search for *CCR* at the top right hand of the screen
	Select the Citi Connectivity Registry Request form

Alternatively, you may access the form directly via this link
(https://cmp.nj.ssmb.com/marketplace/control/product/~productId=31622_331228_GLOBAL#)

Request Type

The CMP form will allow you to request a brand new connectivity or to modify an existing one through a technical update to a Firewall Request. The questionnaire section for both request types require identical information be provided with only slight exception. A technical update will request the existing CCR ID be provided, so that the specialist assigned can link the modification with the existing ID, wile a New Connection does not require this information.

Field	Explanation / Data To Enter

Request Type:

*Request Type

- ○ New Connection {Creation of Entirely New CCR ID}
- ○ Technical Updates {Existing CCR ID: Add, Modify and/or Delete Rules}
- ○ Non-Technical Update {Existing CCR ID: Add or Remove Contacts}
- ○ Termination {Existing CCR ID: Termination of the entire CCR ID and all rules}
- ○ Assistance Request

Type of Connectivity Involved:

*Type of Connectivity Involved

AppSense

(Please select)
Firewall
AppSense
Security Access Control List
Proxy
IP Registration

NOTE: If your connectivity was working before and has recently stopped working then the issue you are experiencing is not related to the CCR application and cannot be addressed by our support team.
This is a break fix situation and requires troubleshooting, proper assignment and potential escalation. If you have not already done so, please open up a ticket with ServiceNow reporting this as a problem and include all SOEIDS and Machine numbers as well as your existing Appsense AD Group name.
For issues with Tectia SSH, MTSC or Attachmate the first contact should be One Touch at THIS LINK. This website grants you access to One Touch support. OneTouch can raise a Service Now support ticket and perform basic troubleshooting. OneTouch notes as many details on the support ticket as possible and if they are unable to resolve, escalate the issue to expert support.

*Request Urgency (Please select) (Please select) BAU Business Critical Emergency	The urgency of your request is determined by the required implementation date and the potential impacts to Citi were the request not implemented.

*Note that requests should not be classified as higher than BAU unless there is a justifiable business reason for doing so.

      BAU: Business As usual – Request will follow normal business SLO for implementation, typically 5 to 10 business days.

      BUSCRIT: Business Critical - Request is classified as critical, rush implementation. BUSCRIT requests require answering business critical questions and Managing Director approval. BUSCRIT SLO 3 to 5 business days.

      EMER: Emergency - Requests are classified as an emergency due to a break/fix of a production failure. EMERs require a ticket in ServiceNow, CT, or EMS, an emergency justification and Managing Director approval.

      Please Note: Business Critical requests require Managing Director approval. EMERs require MD Approval and an EMS ticket number.) |
| **Project Sector:**

* Project Sector (Please select) (Please select) Corporate Center CTI GCB ICG | Select the Sector of the business who will own the connectivity. |
| **Project Region:**

*Project Region (Please select) (Please select) ASPAC EMEA JAPAN NORTH AMERICA LATAM MEXICO | Select the region where the Business resides and the majority of the business activity will reside. |

Connectivity Justification **By audit requirement it is critical that you provide sufficient details around the BUSINESS JUSTIFICATION for the connectivity you are requesting.**	All change request must have business details providing an explanation as to why the connection is required. Please provide a clear and documented benefit to Citi businesses or customers. The connectivity must be legally permissible, have ISO approval and be represented by a Citi Employee. Attempt to provide answers to all of the following questions.. What business processes and owners of these processes are being supported? What systems and or applications are used in this process? Is this a new process or a change to an existing process or service? Please make sure to include Citi SOW number(s) if applicable, any other supporting details. Note: Requests containing insufficient detail will result in delay of processing of the request or cancelation. * All Merger / Acquisitions / Divestitures must have an active Transition Services Agreement (TSA) for all requests..

Business Case

Field	Explanation / Data To Enter
ServiceNow Business CAB Approver Group/Code. Supplying the Business CAB Approver Code may help reduce the number of approvers required	Please provide a ServiceNow Business CAB RFC Approver Code. Supplying the Business CAB RFC Approver Code may help reduce the number of RFC approvers required.. You can look them up here: RFC CAB Approver Codes . Please select your choice ONLY from the "ID" column
Do not implement before Do not implement before [ ]	Populate with a date when there is potential risk associated to the connection if it were to be implemented prior to a certain date. For example, if a contract between Citi and a Third Party indicates data transfer is not to commence before 5/1/2013, then this date should be provided here.
Requestor - (must be Citi employee/FTE): * Requestor - must be Citi Employee/FTE No Value Set Update	Enter the SOEID of the Citi FTE (full time employee) who is requesting connectivity.
Business Owner-Primary: *Business Owner - Primary No Value Set Update	Enter the SOEID of the Citi FTE (full time employee) who will be responsible for connectivity. Note: The Primary business owner will be responsible for providing connectivity details, confirmations, and completion of annual connectivity verification reviews.

Business Owner-Secondary: *Business Owner - Secondary No Value Set [Update]	Enter the SOEID of the Citi FTE (full time employee) who will be a back up or secondary resource for the connectivity. Note: The Secondary business owner will be able to providing connectivity details, confirmations, and completion of annual connectivity verification reviews.
Project Coordinator: *Project Coordinator No Value Set [Update]	Enter the SOEID of the individual who is submitting the request on behalf of the business or managing the Connectivity Project. This individual will have no ownership of the connection, but will be utilized as a resource for project and connectivity details.
ISO: *ISO [Look Up]	Enter the SOEID of the Business Information Security Officer responsible for verifying the business request requirements when needed.. If you do not know the BISO, please contact the business manager for assistance. Otherwise you may use the Locate Your BISO tool located here (http://www.citigroup.net/informationsecurity/locate_biso.htm). An ISO will no longer be notified or required to review/approve new connectivity requests or changes to connectivity requests. You should however be aware that an ISO contact will continue to be collected for every connection request record. You will receive an automated system e-mail notifying you have been selected as an ISO contact for a connection request, and provide you the opportunity to opt out if this selection was made in error. Reasons an ISO contact is required for a connectivity request record are as follows: • In the event that the External Connectivity Analyst needs to contact you about the change requested in the record. • As an escalation point for the Annual Connectivity Verification (ACV) process where the business owner has been unresponsive. • As an escalation point in the Buscrit/EMER or Temporary Approval process where the business owner has been unresponsive. Any ISO (BISO, TISO, or GISO) who supports the business can be selected.

| Business Tester: | Enter the SOEID of the business contact responsible for testing, or coordination of the testing, of the connectivity once it has been implemented. The tester will be listed on the RFC and will be required to provide confirmation of his successful testing.

The tester can be the same as the Primary/Secondary owner. |
| --- | --- |
| **Business Tester:**

*Business Tester

No Value Set

Update | |

Third Party Details

This section of the Marketplace form is used to obtain information regarding Third Party vendors. All proxy requests need to have this information populated.

Field	Explanation / Data To Enter
Vendor Contractual Statement of Work Vendor Contractual Statement of Work Remaining characters: 255	Enter the Vendor contractual Statement of Work (SOW) number associated with the connectivity request. This will be used for review of the project details, connectivity tracking, and Entitlement reviews.
Third Party Company Name: *Third Party Name	Provide the name of the Third Party organization who will be utilizing the connectivity that requires access through the Firewall
CASP Supplier ID: *CASP Supplier ID	Enter the CASP [Citi Approved Supplier Program] Supplier number associated with the third party vendor.

This information may be obtained by querying the CASP database.(https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)

A CASP Supplier ID must be obtained and entered before a Third Party firewall modification can be processed. If the third party has not been registered in CASP please review the process requirements in the FAQ (https://casp.ny.ssmb.com/casp/popups/file.asp?filename=FAQ.doc&ID=0) |

CASP Detail ID:	Enter the CASP [Citi Approved Supplier Program] Detail ID corresponding to the Supplier and Business relationship.
* CASP Detail ID	This information may be obtained by querying the [CASP database.](https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)
	A CASP Detail ID must be obtained and entered before a Third Party firewall modification can be processed. If the third party has not been registered in CASP please review the process requirements in the [FAQ](https://casp.ny.ssmb.com/casp/popups/file.asp?filename=FAQ.doc&ID=0)
Third Party Contact Name: *** Third Party Contact Name**	Enter the name of the contact person at the Third Party. This information can be obtained from the CASP Procurement Manager listed for the Third Party in [CASP database.](https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)
Third Party Contact Type: *** Third Party Contact Type** (Please select) Relationship Manager Supplier Third Party Contact Technical Support	Select the current role of the contact at the third party.
Third Party Contact Phone: *** Third Party Contact Phone**	Enter the phone number of the contact person at the Third Party. This information can be obtained from the CASP Procurement Manager listed for the Third Party in [CASP database.](https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)
Third Party Contact E-mail: *** Third Party Contact E-Mail**	Enter the Email Address of the contact person at the Third Party. This information can be obtained from the CASP Procurement Manager listed for the Third Party in [CASP database.](https://casp.ny.ssmb.com/casp/asp/vendor_locator.asp)

Technical Details

Field	Explanation / Data To Enter

Please estimate how frequently this connectivity will be used *Please estimate how frequently this connectivity will be used Biweekly (Please select) Daily Weekly Biweekly Monthly Bimonthly Quarterly Semi-Annual Annual As-needed (no set schedule, example: COB)	Select the data frequency
Indicate the type and highest classification of data being accessed with this connectivity. Data must be encrypted end to end if it is Confidential or Higher *Customer Data (Please select) (Please select) Public Internal Confidential Restricted Not Applicable *Citi Data (Please select) (Please select) Public Internal Confidential Restricted Not Applicable	Select the classification that best corresponds to the data that is being transferred. **Confidential:** Information that Citi Businesses are obligated to protect including, but not limited to information belonging to: customers, Workers, Third Parties, or Citi Businesses. Any combination of data subject to regulatory or contractual restrictions on disclosure. Information that the Business determines has the potential to provide a competitive advantage or have a significant impact on the Business if disclosed to unauthorized individuals. **Internal:** Information that is commonly shared within Citi is not intended for distribution outside Citi and is not classified as Restricted or Confidential. **Public:** Information that is freely available outside of Citi or is intended for public use by the Information Owner. **Restricted:** Information that, if disclosed to unauthorized individuals, could have a significant impact on Citi's legal or regulatory obligations or on its financial status, customers or franchise. **N/A:** No Data will be transferred.
*Does an AD group exist for this request? (Please select) (Please select) Yes No	Indicate whether an Active Directory group, containing the members you wish to whitelist with this request, already exists.

If an Active Directory group does not exist, you must first have the AD group by ordering this product. You can come back to submit your AppSense request as soon as your AD group is created

*Active Directory Domain No Value Set Look Up	Once the Active Directory has been created, use the lookup functionality to find and select the group name/id.
How would you like to find the Active Directory group? * How would you like to find the Active Directory group? (Please select) Find by group name Find by group owner or sponsor Find by group description Find by group member	Select the option in which you would like to find the Active Directory Group
Please specify the types of applications to add to whitelist *Please specify the types of applications to add to whitelist ☐ Black-listed Application ☐ CSI Application ☐ Non-CSI Application	Select the type that best corresponds to the application access the third party will require. If the Third Party requires access to multiple applications, please select all applicable types. • Black-listed application: An application that is in the AppSense default blacklist • CSI Application: An application that is listed in CSI • Non-CSI Application: An application that is not listed in CSI
Do you want to unblock ports? *Do you want to unblock ports? Yes (Please select) Yes No	Does the Third Party require access to a specific port? Yes/No
Yes	**Please complete this spreadsheet with the list of ports required:**	Download, populate, and upload the AppSense port template spreadsheet. (https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/Appsense_Ports_Template.xls) Refer to the examples on the document for assistance.

| **Please complete this spreadsheet with the list of affected users:** | Download, populate, and upload the spreadsheet (https://technology.home.citi.net/sites/ctompd/mpd/firewall/Shared%20Documents/AppSense_Users.xls) listing all users that will be affected by this AppSense request.

Refer to the examples on the document for formatting assistance. |
|---|---|

All AppSense requests are considered high risk and therefore require the answering of the following questionnaire.

You may select multiple operating systems by holding down the CTRL key

Does this request include Third Party users who have Administrator access to their TPA desktop?	Indicate whether any of the users in the assigned Active Directory have Administrative access to their machine.
Does this request include Third Party users who have administrator access to destination servers they access via TPA?	Indicate whether any of the users in the assigned Active Directory have Administrative access to the destination servers they access via TPA (Third Party Access).
Are all the hosts accessed by the Third Party users of this request managed by Citi?	Indicate whether all of the hosts are managed/owned by Citi

If using Interactive Access or Tunneling services (for protocol list that includes Interactive Access/tunneling see appendix E OSTIA QRC) please describe how CONTAINMENT of users is achieved at the destination servers being accessed from TPA	Provide justification.
Are there contractual terms of relationship with the Third Party?	Does Citi have a signed legal contract specifying the terms of relationship with the Third Party being affected by this AppSense request? Yes/No
Is Confidential, PII or Restricted Information stored on Citigroup owned devices or on vendor owned devices subject to a contract that is compliant with Citi policies and standards?	Are all the Confidential or higher data elements being accessed by the Third Parties subject to contractual applications forcing Citi Policy and Standard compliance.

Priority Questions

This section of the Marketplace form is required when the connection urgency has been entered as either *Business Critical* or *Emergency* under section *Project Details*. The added details are required for justifying why the request cannot be entered as *BAU (Business as Usual)*.

Field	Explanation / Data To Enter
VT (Sev 1-2), ServiceNow or EMS Number *VT (SEV 1-2), ServiceNow or EMS Number	*#Only required for EMERs#* All Firewall submissions with *Request Urgency* of *Emergency* require an associated Virtual Ticket ServiceNow ID or EMS Number. Emergency requests without a valid number will not be processed.
Provide the name/SOE ID of the approving Senior Managing Director *Provide the name/SOE id of the approving Senior Managing Director No Value Set Update	Use the provided search functionality to find the Managing Director who will provide their approval to proceed with the EMER/BUSCRIT request. Note: The search box is limited to Citi employees with MD or higher title.
What business is requesting the change? *Which business is requesting the change if different from the group raising the RFC?	Populate the business following Global Directory formatting standards.
Which department is the owner of this process? *Which department is the owner of this process?	Populate the department following Global Directory formatting standards.

Describe the business impact if the change does not occur out of cycle. *Describe the impact to the Business if this change does not occur out of cycle. |	Explain, in detail, what negative impact would affect the business and/or Citi as a whole if the firewall modification is not made in an expedited fashion. Provide as much detail as possible, including contract deadlines, financial loss amounts, or penalties. This information will be reviewed, and confirmed, to determine whether your request does, in fact, require expedited handling.
Does any additional business testing need to take place for this unplanned change? *Does any additional Business testing need to take place for this unplanned change? (Provide details) *Remaining characters: 255*	Please note if your business requires testing beyond the normal implementation verification step that will be completed after the firewall change has occurred. Additional business testing can include verification that the destination and source application are compatible and verification that the two applications are running as expected pre-change.
What process failed that prevented this change from being able to follow the normal change cycle?. *What process failed that prevented this change request from being able to follow the standard change cycle?	Explain, in detail, why this request was not submitted to the External Connectivity Management team with sufficient time to undergo the normal change cycle. This information will be reviewed, and confirmed, to determine whether your request does, in fact, require expedited handling.
What other changes, if any, are scheduled during the same time frame? *What other changes, if any, are scheduled during the same time frame for the same or a related environment that may clash with this request? (Provide details)	Provide details on known changes that will be occurring during the time frame you are requesting a firewall change be made. Any changes potentially affecting the source or destination networking environments should be noted.

Additional Information

Please assist the processing team by answering the following optional questions to help in expediting your request.

Field	Explanation / Data To Enter

Other Documentation	Use this option to provide any documentation you would like the reviewer to take into consideration. If you have design documentation from a CTI project request, please include it in this section.
Comments Comments	Use this space to enter any additional information you would like the reviewer to take into consideration

What to Expect Next

Once the CMP request has been completed, the request will be routed to the External Connectivity Management team and a specialist will be assigned to support the request. The External Connectivity Specialist will review the request details and reach out to the submitter for clarification on any incorrect/outstanding items before transferring the request into the Citi Connectivity Registry. If at any time the External Connectivity team reaches out to the business for additional information and no response is received within 14 days, the CMP may be considered closed.

All AppSense exception requests are considered high risk. In order to compensate for the vulnerabilities created by these high risk requests the business will be required to provide information/controls above and beyond that of a regular request.

Action	SLO*
Global Information Security (GIS) Review Once approved by the business and ECM, the request is routed to GIS for review against security standards and OSTIA guidelines. If the request complies with all requirements, it is sent for implementation. If there are any issues, or the request is deemed a high risk, the request is schedule for Working Group review.	1 day
Third Party Working Group Approval All requests marked for review by GIS Review, require a higher level Third Party Working Group Approval. The Third Party Access Solutions Working Group operates under the direction of the Information Security Risk Operating Committee (ISROC) to review connectivity requests that traverse the Citi perimeter. requests TPASWG review happens every Tuesday at 9am ET. Cutoff for each week's review is Monday 12 noon ET for ISO approval completion. Click on the header of this section to obtain additional information on the approval process.	7 days *Historical Median*: 1.3 days
Annual Connectivity Verification 365 days after the Implementation the Primary/Secondary Business Owner [as selected on the original CMP request] will receive an email requesting they complete the Annual Connectivity Verification. You have 90 days to complete the ACV. If the ACV is not completed it will be reported on the monthly report to Senior Management. Click on the header of this section to obtain	Business Dependent 90 Day Max

additional information.	
Notifications Business users assigned to the request as Submitter, Information Security Officer, Business Manager, Project Coordinator, and Technical coordinator will receive email notifications when an action is required. Please ensure that you pay special attention to any emails coming from *OTRM US CCR or containing "CCR Notification" on the subject line. For additional details on the notifications please Notifications section in the appendix.	N/A

Appendices

Roles and Entitlements

The CMP Request will be transferred into the Citi Connectivity Registry system by the ECM Specialist. If the business wishes direct access to CCR to provide required approvals or to take advantage of searching capabilities they may take on the following roles.

CCR Business Roles

The below Roles are Business roles that required to approve a request in CCR or to verify if the request is still required by the business

Role	Functions	CCR Stage
Business User Role	• Able to manage Connection Contacts • Complete the Annual Connectivity Verification (ACV) Process	• Role is needed in order to complete the Annual Connectivity Verification.
ISO	You should however be aware that an ISO contact will continue to be collected for every connection request record. You will receive an automated system e-mail notifying you have been selected as an ISO contact for a connection request, and provide you the opportunity to opt out if this selection was made in error.	An ISO will no longer be notified or required to review/approve new connectivity requests or changes to connectivity requests Reasons an ISO contact is required for a connectivity request record are as follows: • In the event that the External Connectivity Analyst needs to contact you about the change requested in the record. • As an escalation point for the Annual Connectivity Verification (ACV) process where the business owner has been unresponsive. • As an escalation point in the Buscrit/EMER or Temporary Approval process where the business owner has been unresponsive.

Role	Functions	CCR Stage
Business Manager	• Manager of the requestor, with the ability to perform the annual entitlement review for the requestor. • Provides approval in the IP registration workflow; provides approval for requests submitted by non-employees.	• Required role for IP Registrations where the business manager must approve the request
Director	• Managing Director, provides approval for BUSCRIT and EMER requests • Required for all EMER and Buscrit Connections	• Provides director approval for EMER and BUSCRIT via Email response to system notification
Business Tester	• Citi employee responsible for testing the connectivity during the change window; will be identified on the RFC..	• User tests connectivity outside of CCR

Note: Only Citi employees can hold CCR roles

Obtaining Entitlements in CCR

The Citi Connectivity Application requires that appropriate entitlement be granted before any action can be taken. To request entitlement follow the steps outlines below

Access the CMP Product HERE

Select whether you are requesting an addition or removal of role. For the most part, this form will be used for *adding users to a group*	*Do you need to add or remove a user to a g Add user to a group (Please select) Add user to a group Remove user from a group
If you have an existing CCR entitlement and wish to add additional functionality then select Yes. If you do not have any CCR entitlement then select No.	*Are you an existing CCR User (Please select) (Please select) Yes No
The user type is dependent on what type of functionality you require and what business group you belong to. For the most part, you should be selecting	

Business User or Approver. Only individuals on the implementation teams or directly working in the CCR team should use the remaining user types.	***User Type** (Please select) **(Please select)** Business User or Approver Implemention Team ECM / CCR Support

User Type: **Business User or Approver**

Select the role that best fits your requirements **Business User:** Citi Employee or Non-Employee who requires view to complete Annual Connectivity Verification (ACV) attestations. **ISO**: Information Security Officers, BISOs, TISOs, or GISOs; - who will review records and ensures the connectivity complies with security guidelines. **Business Manager:** Citi Employee, who will be the manager approving requests initiated by non-employees.	***CCR Role** ☐ Business User ☐ Business Manager ☐ ISO

User Type: **Implementation Team**

Note: These roles are strictly limited to implementation team members. Entitlement requests will require additional review and approval from the External Connectivity Program. Select the role that best corresponds to the technical business group you belong to.	***CCR Role** ☐ FW Operational Analyst ☐ Proxy Implementer ☐ Appsense Implementer ☐ Global FW Design Engineer ☐ GNO

User Type: **ECM/CCR Support**

Note: These roles are strictly limited to teams responsible for the managing of the Citi Connectivity application. Entitlement requests will require additional review and approval from the External Connectivity Program. **ECM [**External Connectivity Management]: responsible for the creation of CCR records. **OTRM:** Responsible for the review and approval of high risk submissions. **MAD** [Merger mergers acquisitions and divestitures]: Responsible for the review and approval of MAD requests.	***CCR Role** ☐ ECM ☐ OTRM ☐ MAD ☐ TPASWG ☐ ISA ☐ Support Agent ☐ System Administrator ☐ Project Coordinator ☐ Technical Coordinator

TPASWG [Third Party Access Solutions Working Group]
ISA: Responsible for the management of entitlements.
Project Coordinator: Citi Employee representing the business connectivity following a project manager role.
Technical Coordinator: Limited to ECM team members responsible for obtaining, verifying, and entering all technical information into CCR.

The region selection will determine the scope of your role. Please limit your selections only to areas which you are directly responsible for.	*** Region** ☐ ALL REGIONS ☐ NA ☐ EMEA ☐ LATAM ☐ ASIAPAC ☐ JAPAN
The sector selection will determine the scope of your role. Please limit your selections only to areas which you are directly responsible for.	*** Sector** ☐ ALL SECTORS ☐ CORP CTR ☐ CTI ☐ GCB ☐ ICG
Read access will provide the ability to review a record and perform searching functions. Write access is required to approve or edit any record. Users requesting ISO, Business Manager, or any administrative role should select Edit for Permission.	***Permission** (Please select) (Please select) READ WRITE
Finalize the submission by selecting Quick Order or Add to Cart and then hitting submit on the verification page.	Shopping For: **Myself** 🛒 Quick Order 🛒 Add to Cart

The completed requirement request will be sent to your manager for review and approval. After your direct manager has approved the request, you will be automatically granted permission to the system within 2 business days.

For roles falling under User Type: ECM/CCR Support or User Type: Implementation Team, an additional review and approval is required from the External Connectivity program before the access is granted.

System Statuses and Notifications

This section defines the various statuses that can be assigned to a connection request as it is processed through the workflow. The assigned business contacts will be contacted through automated system notifications as the request goes through each process step. This is intended to provide clarification to business users that may receive notifications and/or be reviewing submission status using a Business reporting role.

Activity	Description	Role Responsibility	Email Notifications
Business Justification	The Connection general information is entered.	Project Coordinator	• Request Validation • Rejected • CC'd on Director approval email • Activation Expiration • Business Justification /IP Detail
Technical Architecture	The connection request has been submitted to the Technical Coordinator for input of technical details.	Technical Coordinator	• Technical Architecture • Ostia Update • Verify SOW • Activation Expiration • DE Provide Info – required when additional information is required
Business Manager Approval	The IP Registration request has been submitted to the Business Manager for business review / approval. The connections were created by a non employee and have been submitted for approval	Business Manager	• Receives emails when an IP Registration is submitted • When a non- employee creates a request
MAD Approval	All MAD connections are submitted to MAD approver for review and approval	MAD Approver	• The MAD team is notified when the request is a Merger Acquisition & Divestiture • The requester is also notified when it reaches this
GIS Approval	The connection request has been submitted to the GIS Approver for review and approval.	GIS	• GIS Approvers are notified • Connection Requester is CC'd

TPASWG Approval	The connection request has been submitted to the CCR Admin team for review and approval.	OTRM	• Working Group Approvers are notified • Connection requesters are notified
Implementation Teams	The approved request is routed to the appropriate Implementation teams to review and implement the required changes..	Implementers	• Each Implementation teams are notified • The connection requester is notified when implementation is scheduled and completed
Request Validation	The connection request has been implemented and has received all the necessary approvals.	Project Coordinator	• Connection Requester gets notified
Active	The connection request is active.	Project Coordinator	• Available for Updates

Notifications

Business users assigned to the request as Submitter, Information Security Officer, Business Manager, Project Coordinator, and Technical coordinator will receive email notifications when the record has been updated or an action is required.

Please ensure that you pay special attention to any emails coming from ***OTRM US CCR** or containing **"CCR Notification"** on the subject line.

Exact details of the emails to be received can be viewed below

Information Security Officer Approval	
Subject Line:	CCR Notification: *ID* *Connection Name* BAU Request
Summary	This notification will be sent to the preselected Business ISO
Action Required:	No
Action:	1) Accept Role responsibility as a contact to the connection request

Citi Connectivity Registry

Dear USER,
You have been assigned as a contact on the Citi Connectivity Registry ID listed below. As the assigned contact you are expected to meet certain responsibilities. The breakdown of responsibility by role can be viewed HERE.
If you feel you have been added to this record in error, you may reject the role by CLICKING HERE ; a prepopulated email will appear - simply select the send button.

Assigned Role	ISO
Connection ID	XX
CMP ID	NONE
Requester	XXXX
Region	EMEA
Sector	ICG
Business Unit	Fixed Income
Priority	BAU
Justification	Justification will be provide here for that specific connection request

Note: This is a system generated mail. If you need assistance please contact *IS GLOBAL CCR

Business Manager Approval	
Subject Line:	CCR Notification: *ID* *Connection Name*
Summary	This notification will be sent to the Project Coordinator, Technical Coordinator, ISO, Manager and Business Owner every 365 days after the implementation date or prior verification.
Action Required:	Yes
Responsible Party:	Business Manager
Action:	The business manager approval is "optional" if approval is needed by a Business Manager, you will be notified via email. You will have two options to approve the request 1) You can login to the application to provide approval for the connection and acceptance of risk with its implementation. 2) Use the approval or reject link in the email

Citi Connectivity Registry

citi

Dear USER,

A connectivity request (XXXXX) is awaiting your review and approval/rejection in the Business Manager queue. Please see the details below. We encourage all requests to be reviewed **as soon as possible (not to exceed 1 day** to avoid implementation delays that can negatively impact the lines of business.

The critical connectivity details associated with this ID can be viewed on the attached access form documentation, and at the bottom of this email.

You have the option to approve or reject the connectivity within the Citi Connectivity Registry application here.

Please click here to Approve

Please click here to Reject

Note: This is a system generated mail. If you need assistance please contact *IS GLOBAL CCR

Managing Director Approval	
Subject Line:	CCR EMER-BUSCRIT Expedited request. Approval Action REQUIRED
Summary	Managing Director approval is required for all requests with urgency status of Emergency or Business Critical. This notification will be sent to the Managing Director associated with the record requesting the required approval.
Action Required:	Yes
Responsible Party:	Managing Director
Action:	The Managing Director must reply all to the email providing

their approval or denial of the request.

To:	USER
CC:	USERS
MAIL NOT SENT TO:	
Subject:	CCR XXXXXX EMER-BUSCRIT Expedited request. Approval Action REQUIRED
Sent:	Date Sent

Dear USER,

You are receiving this e-mail because you were named as a Managing Director level approver for a request in the Citi Connectivity Registry (CCR) by USER. Any network Connectivity Request which is created as an EMER/BUSCRIT, must obtain managing director level approval.

CCR ID: XXXXX. 1 (CONNECTION NAME) was defined as an EMER/BUSCRIT.
Business Justification: Citiplex Internal DNS firewall rules - server to server communication - between Citiplex Proxy subnets and the CPOD DNS servers in support of Citi Technology Infrastructure (GNCC)

Please see the questionnaire below. It was completed by the requester, to provide you information as to why this request needs to be expedited for completion.

To approve this request, please click "reply all" to this e-mail and respond with the word, "approved".

If you still have questions about this request, please contact the Project Coordinator Michael Reznick regarding this escalation.

This e-mail was generated by the CCR. If you have general question or comments about it, please e-mail the CCR Service Desk: *IS GLOBAL CCR.

Questionnaire for Director Approval
Provide the name/SOE id of the approving Senior Manager.
Managing Director information goes here
Which Business is requesting the change if different from the group raising the RFC?
Cyber Security Operations / Perimeter Security
Describe the impact to the Business if this change does not occur out of cycle.
DNS team and PSO is scheduling to implement a deny rule to all CPOD DNS. CPOD Subnets need cross connectivity for COB among the DC DNS servers in case of failures.
What process failed that prevented this change request from being able to follow the standard change cycle?
In the event of failure, CPOD proxy server subnets will not be able failover.
Which department is the owner of this process?
DNS Operations
What other changes, if any, are scheduled during the same time frame for the same or related environment that may clash with this Priority 2 request (Provide details)
no
Does any additional Business testing need to take place for this unplanned change? (Provide details)
no

Annual Connectivity Verification	
Subject Line:	CCR Annual Connectivity Verification
Summary	This notification will be sent to the Project Coordinator, Technical Coordinator, ISO, Manager and Business Owner every 365 days after the implementation date or prior verification.
Action Required:	Yes
Responsible Party:	Project Coordinator; Technical Coordinator; ISO; Business Manager; Business Owner
Action:	One of the assigned business contacts must login to the application to verify that the connection is still required.

Citi Connectivity Registry

Dear

You have been listed as the business contacts for the Citi Connectivity Registry Connection ID 74359. This is a reminder that the record is awaiting its annual verification confirming it remains required. According to the Citi Information Security Standard, the business has the responsibility to review and maintain their connectivity records on an annual basis.

The Annual Connectivity Verification (ACV) process was initiated on 03-24-2015 because this connection has not been modified in over 365 days.

The critical connectivity details associated with this ID can be viewed on the attached access form documentation, and at the bottom of this email.

You have the option to validate the connection as still required, or as no longer required, within the Citi Connectivity Registry application here . A step-by-step ACV process guide can be found HERE

Alternatively, only if the connection should be retained, you can provide your response by clicking on the green link below. This will generate a new email that, when sent, will trigger the appropriate action within the application.

Please click here to Confirm the connection is still required

We thank you in advance for your timely response.

Any questions you may have should be directed to *IS GLOBAL CCR

Request Basic Information:

CCR ID	74359.3	**Relationship Name**	ASIAPAC-GCG-Consumer Banking -TIBCO SOFTWARE-GRN
Description	ASIAPAC-GCG-Consumer Banking -TIBCO SOFTWARE-GRN	**SOW Number**	
Region	ASIAPAC	**Sector**	GCB
Business Unit	Consumer Banking	**Activity Description**	Annual Connectivity Verification
ACV Due Date	03-24-2015	**Requested Activation Date**	04-08-2015
CMP ID/ServiceNow ID	WS24125714		

ISO Review

Return to..

Home
Firewall
AppSense
IPReg
Proxy

Information Security Officers (ISOs) are responsible for performing a business information security review and approval of 3rd party network connectivity requests for their business units that are entered into the Citi Connectivity Registry (CCR).

Requests Requiring ISO Review

The following types of network

ISO Review Guidelines

The ISO is responsible for reviewing and approving the request from a **business**

connectivity requests entered into CCR require ISO review:

- 3rd party high risk business-to-business (B2B) connections, including broad access

- 3rd party high risk remote access / IP registrations, including broad access

- Citi internal broad access requests

- Proxy requests

- AppSense requests

- Security ACL requests

- U-Turn requests

Scope of ISO Review

The purpose of the ISO review is to perform signoff on the business justification and business information security of the requested access.

The technical details of the connection will be reviewed by External Connectivity Management (ECM) team if the connection was submitted through them for processing. The ECM team ensures the connection design is acceptably engineered prior to the ISO review. If the connection was not processed through the ECM team, then the ISO should check and verify the technical design of the connectivity with a network engineer.

The Third Party Access Solutions Working Group will perform a risk analysis of all high risk connectivity based on Citi overall requirements. The ISO may consult with the Technical Information Security Officer (TISO) to address any additional business specific security

information security perspective. The following issues should be considered:

☐ Is there a Risk Exception (RE) in place if applicable? **Note**: REs for non-BAU compliant connectivity to the Citi network cannot be executed by the business since the Citi network services the entire corporation. **(CISS 8.1 Sec. 3; CITMS Sec. 3)**

☐ Do the business case details of the request reasonably represent the project need? **(CISS 8.1 Sec. 6.1.1)**

☐ Have the System Security Testing (SST) and Third Party Information Security Assessment (TPISA) processes been completed, scheduled or confirmed to be not required? **(CISS 8.1 Sec. 6.1.1 and Sec. 6.2.3)**

☐ Will the 3rd party access be monitored and controlled by a Citi employee? **(CISS 8.1 Sec. 6.2.1)**

☐ Does the business authorize direct access by the 3rd party? **(CISS 8.1 Sec. 6.2.1)**

☐ If Confidential or Restricted data is being transmitted, does the contract contain a non-disclosure agreement (NDA) that specifically stipulates protection of Citi and Citi customer data? **(CISS 8.1 Sec. 6.2.1)**

☐ Has the NDA been reviewed and signed off by Legal? **(CISS 8.1 Sec. 6.2.1)**

☐ Are there any major weaknesses in the TPISA findings that would make establishing connectivity imprudent? **(CISS 8.1 Sec. 6.2.3)**

☐ If a TPISA was not completed within the past year, does the contract with the 3rd party cover liability issues and information security responsibilities on the part of the 3rd party? **(CISS 8.1 Sec. 6.2.3)**

☐ Do the vendor-managed devices comply with Citi policies and standards? **(CISS 8.1 Sec. 6.2.3)**Have all procedures and requirements for external access to Citi been followed? **(CISS 8.1 Sec. 6.2.3)**Is the data being transmitted properly classified? **(CISS 8.1 Sec. 7.2.1 and Appendix A1)**

☐ Are there conflict of interest concerns? **(CISS 8.1 Sec. 10.1.3)** Note: Consultants may take on a data entry role for a request, provided the request does not relate to the company employing the consultant.

requirements.   However, the ISO is not responsible for either approving either the technical design or analyzing the risk of the connection to the Citi network.

☐ Have all documents uploaded in the Documents section of the request Review Page been reviewed to ensure that proper Design Diagrams are included? (For example, Letters of Notification from Legal should be included with U-Turn requests.) **(CISS 8.1 Sec. 10.2.3 Sec. 10.8.5)**

☐ Is the connectivity requestor a representative of the business unit? Should the requestor be representing the business unit to raise the request? Is the requestor a full time employee of the business? **(CISS 8.1 Sec. 10.2.3)**

☐ Is the request justified by a business need, contract, or Statement of Work (SOW)? **(CISS 8.1 Sec. 10.2.3)**

☐ Does the application adhere to the applicable encryption requirements? **(CISS 8.1 Appendix A1)**

Citi Information Security Standards for ISOs

Information Security officers are responsible for the following requirements in Citi Information Security Standards (CISS):

IT Policy / Standard Exception Process (CISS 8.1 Sec. 3): Exceptions must be managed in accordance with the requirements as set forth in CITMS Section 3 – "IT Policy / Standards Exception Process".

Management commitment to information security (CISS 8.1 Sec. 6.1.1): Citi Businesses must periodically assess its business operations for compliance Standards, Technical requirements, and procedures that ISROC may require. Refer to the following documents for details:

- IS Risk Assessment (ISRA) Process
- Third Party IS Assessment (TPISA) Process
- Application IS Review Process (ISRP)
- IT Risk Control Applicability Matrix (IRCAM-ISRP)
- System Security Testing (SST) Standard
- Citi Infrastructure Vulnerability Assessment (CIVA)

Identification of risks related to external parties (CISS 8.1 Sec. 6.2.1): Citi Businesses must maintain appropriate security of Citi's Information and Information Systems that are accessed, processed, disposed, or managed by Third Parties. Businesses must ensure the security of Citi Information and Citi Information Systems.

Before establishing connectivity with a 3rd party, the Business must:

- Complete a Third Party Information Security Assessment
- Must follow the System Security Testing (SST) Standard to ensure that vulnerability assessments are performed

Addressing security in third party agreements (CISS 8.1 Sec. 6.2.3): When access to Citi Information will be given to Third Parties outside of Citi facilities and management oversight, Information Security requirements where appropriate must be addressed in a documented agreement with the Third Party following processes established in Citi's Vendor Selection and Management Policy and Standards (CSSMP).

Classification Guidelines (CISS 8.1 Sec. 7.2.1): Information Owners must classify Citi Information under their control as one of the following Information Classifications:

- Restricted
- Confidential
    a. Confidential PII – Must comply with confidential classification as well as additional requirements for PII
- Internal
    b. Internal PII – Must comply with internal classification as well as additional requirements for PII
- Public
- Authentication

Monitoring and review of third party services (CISS 8.1 Sec. 10.2.2): Citi Businesses must ensure that Third Parties (excluding customers accessing their own information) that store, process, manage or access Citi Information (except Internal and Public Information), host Citi branded Internet facing applications, or have connectivity to Citi's network resources comply with the applicable sections of the CISS or provide equivalent controls.

Managing changes to third party services (CISS 8.1 Sec. 10.2.3): External network connectivity that provides Third Party access to Citi resources requires management to ensure, either annually or when the Third Party status or access has changed, that the access accurately reflects the current status of the Third Party relationship.

- The Business is responsible for maintaining all information regarding the relationship, including legal contracts and responsible for communicating material changes of the relationship to the Citi Infrastructure provider.

Network controls (CISS 8.1 Sec. 10.6.1): Networks must be protected from threats and security must be maintained for the Information Systems using the network. This includes information in transit across the network.

Business information systems (CISS 8.1 Sec. 10.8.5): Network connectivity between Citi and Third Parties must follow ITPC-approved Technical Standards for Inter-Corporation Connectivity. Each Business and Technology Manager must ensure that all IP connections to Third Parties are protected by Citi Technology and Infrastructure (CTI) managed firewalls.

Segregation in networks (CISS 8.1 Sec. 11.4.5): Management must ensure that Information Systems are segregated on the Citi network in accordance to controls which will limit access to the Citi network.

Network connection control (CISS 8.1 Sec. 11.4.6): For shared networks, especially those extending across the organization's boundaries, the capability of Users to connect to the network must be restricted. Network connectivity must be as limited as possible and follow the Network Security Standard.

Appendix A.1: Encryption Requirements (CISS 8.1 Sec. Appendix A.1): Transmissions involving Confidential PII or higher information, encryption must be performed on an application-to-application / server to server basis; responsibility of the Application manager. In other cases (e.g., individual email, file transfer, etc.) the Business/User is responsible for compliance.

- **Third Parties:** Third Parties who store or process Confidential or Restricted information must either meet the requirements of these Standards or provide comparable controls validated by

an IS assessment and accepted by the Business. (Such information must be encrypted in transit to and from the Third Party when sent electronically.)

Policy, Standards, and Guidelines:

Approved Application Development Security Products
https://archcntr.nam.nsroot.net/archcntr/tools/ctc/Products/Products.aspx?Tab=2&CategoryID=110&OrganizationID=0

Approved Security Management Products
https://archcntr.nam.nsroot.net/archcntr/tools/ctc/Products/Categories.aspx?Tab=2&OrganizationID=0&domainid=907

CATE Appsense Management Suite
https://catecollaboration.citigroup.net/domains/ci/sbc/techstdshmpgs/appsensemanagementsuite.aspx

CATE Server Based Computing Site Includes data on Citrix, Appsense, Sun SGP, VDI, Thin Clients, etc…
https://catecollaboration.citigroup.net/domains/ci/sbc/default.as

Citi Cyber Intelligence Center News Letter
http://www.citigroup.net/informationsecurity/cicid.htm

Citi Desktop Standards:
https://catecollaboration.citigroup.net/domains/ci/cce/hw/desktops/Desktops.aspx
Citi Desktop Software Standards:
https://globalconsumer.collaborationtools.consumer.citigroup.net/sites/CATECB/Lists/Convergence%20Build%20Standards/Latest%20Builds.aspx

Citi Information Technology Management Policy
(CITMP) https://technology.home.citi.net/sites/itpolicylib/docs/CITMPolicy.pdf

CITI Information Technology Management Standards (CITMS)
https://technology.home.citi.net/sites/itpolicylib/docs/CITMS.pdf

Citi Information Security Standards
https://technology.home.citi.net/sites/itpolicylib/docs/CISS.pdf

CitiSFT:
CitiSFT Standards Site:
https://catecollaboration.citigroup.net/domains/security/isp_standards/dpstds/stdshmpgs/CitiSFT.aspx
CitiSFT Support Site:
https://globalconsumer.collaborationtools.consumer.citigroup.net/sites/GSO/citisft/default.aspx

CTI Global Operations Vulnerability Assessment Site:
http://www.citigroup.net/ti/securityOperations/vulnerabilityAssessment.htm

CTI Global Financial Control Product Cards:
http://www.citigroup.net/ti/financialcontrol/

CTI Technology Infrastructure Systems and Tools Directory:
http://www.citigroup.net/ti/systemsDirectory.htm

Contingent Workers, Guidelines for
https://catecollaboration.citigroup.net/domains/ci/ras/Policies%20and%20PCMs/Contingent_Worker_Guidelines.pdf
"Contract staff guidelines" exist under section DS2.4. And the different types of Contract staff are
documented under section AI5.2.6.2. in the following document:
https://internationaltechnology.citigroup.net/APAL/Document%20Library/ITO%20L3%20Procedures.pdf

Continuity of Business Policy Standards
http://www.citigroup.net/citibanknacob/Cob/Documents/OBC%20Policies/CoBStandard%202.0.pdf

Infrastructure Security Products Standards
https://catecollaboration.citigroup.net/domains/security/isp_standards/default.aspx

Infrastructure Security Risk Operating Committee Charter
http://www.citigroup.net/informationsecurity/data/policy/ISROCCharter.pdf

ITPC: Approved Cryptographic Algorithms
http://www.citigroup.net/informationsecurity/data/policy/ApprovedCryptographicAlgorithms.pdf

ITPC: Approved Security Protocols
https://technology.home.citi.net/sites/itpolicylib/docs/ASP.pdf

Key Management Standard
https://technology.home.citi.net/sites/itpolicylib/docs/KMS.pdf

IT Policy/Standard Exception Process
http://www.citigroup.net/informationsecurity/data/policy/ITPSE_Procedures.pdf

Network Security Standard
https://technology.home.citi.net/sites/itpolicylib/docs/NSS.pdf
Network Security Standards Level III Support Document
https://catecollaboration.citigroup.net/domains/security/sid/tpae/Shared%20Documents/Network%20Security%20Standards%20Level%20III/NSS%20Level%20III%20Support%20Doc%20V1.0.pdf

Password Management Technical Standards
https://catecollaboration.citigroup.net/domains/security/appsec/Application%20Security%20Standards/Domain%20Standards/Password%20Management%20Technical%20Standards.pdf

Password Management Technical Standards
https://catecollaboration.citigroup.net/domains/security/appsec/Application%20Security%20Standards/Domain%20Standards/Password%20Management%20Technical%20Standards.pdf

Pointsec for PC and Pointsec Protector Support Site:
https://catecollaboration.citigroup.net/domains/security/isp_standards/hsestds/hsehomepages/Pointsec.aspx

Pkware SecureZip Support Site:
https://catecollaboration.citigroup.net/domains/security/isp_standards/dpstds/stdshmpgs/File%20Security.aspx

Remote Access Standards External Vendor Onboarding
https://catecollaboration.citigroup.net/domains/ci/ras/default.aspx

Secure Email Site:
https://catecollaboration.citigroup.net/domains/security/isp_standards/dpstds/stdshmpgs/Secure%20E-Mail.aspx

System Security Testing Standard
https://technology.home.citi.net/sites/itpolicylib/docs/SSTS.pdf

Tectia Support Site:
https://catecollaboration.citigroup.net/businesssupport/cao/riskmgmt/CSB/Forms/AllItems.aspx?RootFolder=%2fbusinesssupport%2fcao%2friskmgmt%2fCSB%2fSSH%20Tectia&rowid=712

Third Party Information Security Assessment Process
https://globalconsumer.collaborationtools.consumer.citigroup.net/sites/tpisaportal/docs/Documents/TPISA-Proc_v4-2_FINAL_25-Jan-2011.pdf
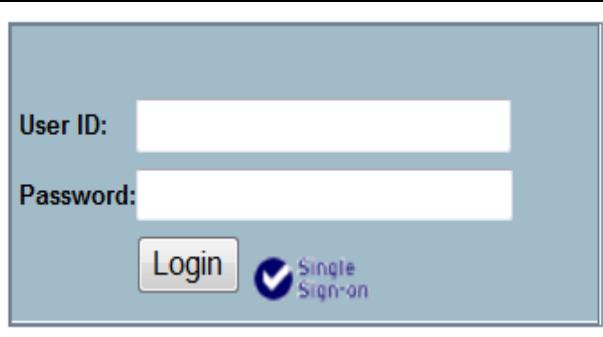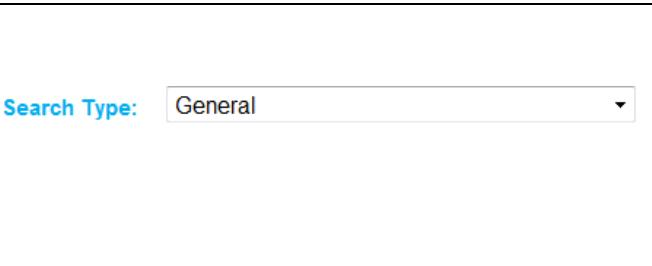
Training and Awareness Programs:
http://www.citigroup.net/informationsecurity/ace_index.htm

Searching for a Record within CCR

It is normally not required, nor permitted, for a business contact to access the Citi Connectivity Registry application; however, in certain cases, such as Information Security Offers reviewing/approving a request; Primary/Secondary owners performing Annual Connectivity Verification; or an authorized business user searching for record status it is required to search through the application. The steps detailed below provide guidance on how to search the application for an individual record.

*Appropriate entitlements should be obtained prior to attempting a search.

User ID: [ ] Password: [ ] Login ✔ Single Sign-on	**Log into CCR application using your Single Sign On (SSO) ID.**
Citi Connectivity Registry INBOX SEARCH MY CONNECTIONS	**Select Search on the top left hand of the page**
Search Type: General ▼	**For business users, the Search Type should remain as "General"**
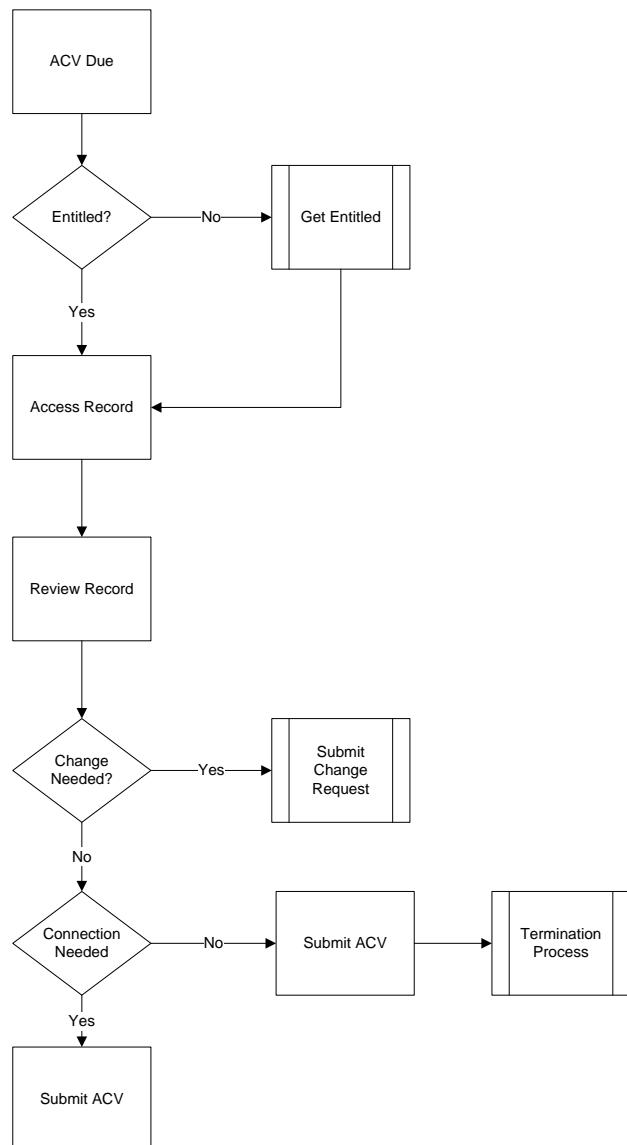
Search Type: General ▾ Process ID 46830 Version Relationship ID Requester (SOE ID)	**Use the available fields to search for the required record. The most appropriate search fields are Process ID; Relationship ID; Requester; and Relationship Name.**
Search Results ID Name Activity ⊙ 60523.1 BrianTest1 Business Justification Update Terminate Manage	**Select the Corresponding Record and Select Update**

Annual Connectivity Verification

Annual Connectivity Verification (ACV) is initiated when a connection has been fully implemented for over 365 days. The ACV process provides an auditable confirmation from the business that the implemented connectivity continues to be required, that the original justification and statement of work remains current and that all contact information is still accurate. This confirmation and validation serves to meet requirements set forth in the Citi Information Security Standards.

Workflow

```
                    ┌─────────────┐
                    │   ACV Due   │
                    └──────┬──────┘
                           │
                           ▼
                      ◇ Entitled? ◇ ──No──→ ┌──────────────┐
                           │                │ Get Entitled │
                          Yes               └──────┬───────┘
                           ▼                       │
                    ┌─────────────┐◄───────────────┘
                    │Access Record│
                    └──────┬──────┘
                           │
                           ▼
                    ┌─────────────┐
                    │Review Record│
                    └──────┬──────┘
                           │
                           ▼
                    ◇Change Needed?◇ ──Yes──→ ┌──────────────┐
                           │                  │    Submit    │
                          No                  │    Change    │
                           ▼                  │   Request    │
                    ◇ Connection ◇            └──────────────┘
                    ◇   Needed   ◇ ──No──→ ┌──────────┐    ┌─────────────┐
                           │               │Submit ACV│──→ │ Termination │
                          Yes              └──────────┘    │   Process   │
                           ▼                               └─────────────┘
                    ┌─────────────┐
                    │ Submit ACV  │
                    └─────────────┘
```

Prerequisites

The Citi Connectivity Application requires that appropriate entitlement be granted before any action can be taken. To request entitlement follow the steps outlines below

Access the CMP Product HERE

Select whether you are requesting an addition or removal of role. For the most part, this form will be used for *adding users to a group*	***Do you need to add or remove a user to a g** Add user to a group (Please select) Add user to a group Remove user from a group
If you have an existing CCR entitlement and wish to add additional functionality then select Yes. If you do not have any CCR entitlement then select No.	***Are you an existing CCR User** (Please select) (Please select) Yes No
The user type is dependent on what type of functionality you require and what business group you belong to. For the most part, you should be selecting Business User or Approver. Only individuals on the implementation teams or directly working in the CCR team should use the remaining user types.	***User Type** (Please select) (Please select) Business User or Approver Implemention Team ECM / CCR Support

User Type: **Business User or Approver**

Select the role that best fits your requirements **Business User:** Citi Employee or Non-Employee who requires view to complete Annual Connectivity Verification (ACV) attestations. **ISO**: Information Security Officers, BISOs, TISOs, or GISOs; - who will review records and ensures the connectivity complies with security guidelines. **Business Manager:** Citi Employee, who will be the manager approving requests initiated by non-employees.	***CCR Role** ☐ Business User ☐ Business Manager ☐ ISO

User Type: **Implementation Team**

Note: These roles are strictly limited to implementation team members. Entitlement requests will require additional review and approval from the External Connectivity Program. Select the role that best corresponds to the technical business group you belong to.	***CCR Role** ☐ FW Operational Analyst ☐ Proxy Implementer ☐ Appsense Implementer ☐ Global FW Design Engineer ☐ GNO

User Type: **ECM/CCR Support**

Note: These roles are strictly limited to teams responsible for the managing of the Citi Connectivity application. Entitlement requests will require additional review and approval from the External Connectivity Program. **ECM [**External Connectivity Management]: responsible for the creation of CCR records. **OTRM:** Responsible for the review and approval of high risk submissions. **MAD** [Merger mergers acquisitions and divestitures]: Responsible for the review and approval of MAD requests. **TPASWG** [Third Party Access Solutions Working Group] **ISA:** Responsible for the management of entitlements. **Project Coordinator**: Citi Employee representing the business connectivity following a project manager role. **Technical Coordinator**: Limited to ECM team members responsible for obtaining, verifying, and entering all technical information into CCR.	***CCR Role** ☐ ECM ☐ OTRM ☐ MAD ☐ TPASWG ☐ ISA ☐ Support Agent ☐ System Administrator ☐ Project Coordinator ☐ Technical Coordinator
The region selection will determine the scope of your role. Please limit your selections only to areas which you are directly responsible for.	*** Region** ☐ ALL REGIONS ☐ NA ☐ EMEA ☐ LATAM ☐ ASIAPAC ☐ JAPAN

The sector selection will determine the scope of your role. Please limit your selections only to areas which you are directly responsible for.

* Sector

☐ ALL SECTORS
☐ CORP CTR
☐ CTI
☐ GCB
☐ ICG

Read access will provide the ability to review a record and perform searching functions.

Write access is required to approve or edit any record. Users requesting ISO, Business Manager, or any administrative role should select Edit for Permission.

* Permission

(Please select)
(Please select)
READ
WRITE

Finalize the submission by selecting Quick Order or Add to Cart and then hitting submit on the verification page.

Shopping For: **Myself**

🛒 Quick Order   🛒 Add to Cart

The completed requirement request will be sent to your manager for review and approval. After your direct manager has approved the request, you will be automatically granted permission to the system within 2 business days.

For roles falling under User Type: ECM/CCR Support or User Type: Implementation Team, an additional review and approval is required from the External Connectivity program before the access is granted.

Accessing the Record

Login to the CCR website
https://connectivityregistry.citi
group.net

Username: kt03862

Password: •••••••••••

Sign On

Single Sign-on   Change Password   Reset Password

Review, and accept, the system terms of use.	**Citi Connectivity Registry** You are authorized to use this System for approved business purposes only. Use for any other purpose is prohibited. All transactional records, reports, email, software and other data generated by or residing upon this System, to the extent permitted by local law, are the property of Citigroup Inc. or one of its subsidiaries or their affiliates (individually or collectively 'Citigroup') and may be used by Citigroup for any purpose authorized and permissible in your country of work. Activities on this System are monitored to the extent permitted by local law. [Accept] [Declin...]
Click the Show Filters link	**View:** 22:55:02 ▼ **Show filters** ☐ ID ▼ Description
Select Processes	Select processes FW ACV Process and ACV Run **Processes** Available processes Selected processes Auto Push ➡ FW ACV Process FW Data Entry ➡ FW ACV Run FW DE Data Entry FW Expiration Review ⬅ FW Fireflow Process ⬅⬅ FW ISO Review
Add Condition for ID	Enter the ID found on the subject line of the email notifying you of ACV requirement **Conditions:** ID ▼ Add condition ☐ Case sensitive ID is ▼ 12345
Enter the record in edit mode	Select the play button at the end of the search result | ☐	ID	Description	Activity	Phase	Task Partic...
---	---	---	---	---	---
☐	49518	NA GCG ITO TCS GRN	Verify SOW	ACV	Unassigned	

Reviewing the Record

The reviewer is responsible for ensuring that the record information remains accurate. In order to accomplish this, you should review the business justification; statement of work; target contacts; and technical details.

These data elements can be found by perusing the tops at the top of each record.

Business Justification	Can be found under tab "Business Justification" section "Business Case"
Statement of Work (SOW)	Can be found under tab "Business Justification" section "Business Case"
Target Contacts	Can be found under tab "Business Justification" section "Target Contacts"
Technical Details	Can be found under tab "Implementation". The section will be dependent on the type of request; the most common request type – Firewalls - will have the technical details under "FAF".

If any item is outdated and requires a modification, please see section "Updating Record" on this document. Record modifications should be submitted after inputting approval comments as outlined on the next section.

Approval Input

After you have performed the review of connection details, you should return to the Approver Input page and certify whether the connection is required.

On the top of the page select Submit Activity then select whether the connection is required, enter comments, and action the request to "Next Participant"

Updating Record

If, during the record review, you discovered an item requiring a modification please submit a new Citi Market Place order accordingly. You may use the CMP form "Citi Connectivity Registry Request" to submit the request

https://cmp.nj.ssmb.com/marketplace/control/product/~productId=31622_331228_GLOBAL#

OSTIA Questionnaire

Return to..
Home
Firewall
Proxy
IP Reg

All submitted transfers considered High Risk, either because they meet automatic triggers or after a manual review, will require the submission of the below questionnaire.

Generic Risk Questions: All connectivity triggering GIS review will require an answer to these questions.

1. Operating Systems: (Example – Windows 2003)

2. Is Antivirus Installed? □ Yes □ No □ Other (If Other, give explanation)

3. Intrusion Detection System Used? □ Yes □ No □ Other (If Other, give explanation)

4. Is Audit Logging Used?   □ Yes □ No □ Other (If Other, give explanation)

5. Is Audit Logging Controlled by Citigroup?   □ Yes □ No □ Other (If Other, give explanation)

6. Requires split tunneling?   □ Yes □ No □ Other (If Other, give explanation)

7. Is this host Citigroup owned or owned by the 3rd party: □ Citi   □ 3rd Party

8. Is Confidential, PII (Personally Identification Information) or Restricted Information accessed by anyone using the proposed connection? (Either on a Citi device or Citi Confidential PII/Restricted information on a 3rd party device?) □ Yes □ No □ Other (If Other, give explanation)

If the confidential or higher information will be accessed by a third party

8a. If owned by the 3rd party, does the contract specifically stipulate adherence to Citigroup policies and standards? □ Yes □ No □ Other (If other, give explanation)

8b. Describe how the device on the non-Citigroup end of the connection complies with the Citigroup Information Security standards: (Give Explanation)

Generic Containment Question:

This question is only applicable to connections containing ports TCP/UDP 69 TFTP;TCP/UDP 135 DCE;UDP/137 Netbios;UDP/138 Netbios;TCP/UDP 139 Netbios;UDP/161 SNMP;UDP/162 SNMP-trap;TCP/445 MS Directory Services;TCP/512 Rexec;TCP/513 Rlogin;TCP/514 Rshell;TCP/3389-3391 RDP;TCP/UDP 4899 RAdmin;TCP/UDP 6502 NetOp Remote Control

Describe the control environment at Citigroup destination system and the containment strategy to keep permitted access to the destination servers or within the approved network segments

Specific Questions dependent on Port/Service

Port		Question	Responses
TCP / 20 FTP	#1	Is requested connectivity will be used for:	FTP
			FTPS
			Other
	#2	For FTP or FTP-S port 20 is not needed. For other describe the usage.	Text Box
TCP/21 FTP	#1	Select the service the connectivity will be used for:	FTP
			FTPS
			Other
	#2	For FTP-S define the data channels to be configured. For Other Describe the usage.	Text Box
	#3	For FTP or FTP-S define how authentication and data transmitted will be encrypted.	Text Box
TCP/22 SSH/SFTP	#1	What service will be utilizing TCP_22	SSH
			SFTP
			Other
	#2	If selecting other as the service, explain the connectivity	Text
	#3	Describe the control environment at Citigroup destination system and the containment strategy to keep permitted access to the destination servers or within the approved network segments, by selecting all that apply:	Application GUI
			Secure Shell: with Whitelist/ Blacklist **Must provide a copy of the Whitelist/Blacklist
			GSF - Select all that apply
			CA Audit
			ESM Agent
			KDC/LDAP
			PAR Client
			PowerBroker
			SafeWord Cleint
			SCpier

			Sun IDM
			Other
			N/A-SFTP file transfer only
	#4	If selected <u>Other</u> as the control detail, explain the connectivity	Text
	#5	Select the application or product used for the SFTP file transfers.	Tectia
			Tumbleweed
			Other
			N/A - SSH only
	#6	If selected <u>Other</u> as the file transfer application, explain the connectivity	Text
TCP/23 Telnet	#1	Describe the control environment at Citigroup destination system and the containment strategy to keep permitted access to the destination servers or within the approved network segments, by selecting all that apply:	Secured by OS
			zLinux
			zVM
			AS/400
			zVSE
			MVS
			OS/390
			other
	#2	If selecting other, explain the connectivity	Text
TCP/25 SMTP	#1	All SMTP servers listed in the request are managed by Citi Global Messaging?	Yes
			No
TCP/UDP 53 DNS	#1	Are these connections to the authorized inbound/outbound DNS servers?	Yes
			No
TCP /80 HTTP	#1	Does this connectivity require passing authentication data?	Yes
			No, This is a redirect to a secure protocol
	#2	If yes, What is the encryption used to secure the authentication data	text
TCP /81 HTTP	#1	Does this connectivity require passing authentication data?	Yes
			No, This is a redirect to a secure protocol

		If yes, What is the encryption used to secure the authentication data	text
	#2		
TCP/UDP 109 POP2	#1	Is this for POP Protocol?	Yes
			No
	#2	If No, What service will be using the port?	text
TCP/UDP 110 POP3	#1	Is this for POP Protocol?	Yes
			No
	#2	If No, What service will be using the port?	text
TCP/111 SunRPC/NFS	#1	What service is utilizing TCP_111?	NFSv4
			NFSv3 or below
			Unix RPC
			Other
	#2	Provide the versions used, explaining the port requirements.	Text
		If NFSv4, TCP_2049 must be used.	
		If NFSv3: Can the RPC ports be statically defined?	
	#3	If selecting other, explain the connectivity	Text
TCP 115 Simple FTP	#1	Do you mean SSH/Secure File Transfer?	Yes: Use tcp/22
			No
	#2	If No, What service will be using the port?	text
TCP/222 RSHD	#1	Describe the control environment at Citigroup destination system and the containment strategy to keep permitted access to the destination servers or within the approved network segments. Explain what service will be using the connectivity and why it is being used. Is this connectivity for RSH?	text
TCP/443 HTTPS/SSL	#1	Will this connectivity be used for Web Service	Yes
			No

	#2	If No, explain the connectivity:	Text
TCP/593 HTTP RPC	#1	Describe the control environment at Citigroup destination system and the containment strategy to keep permitted access to the destination servers or within the approved network segments. Explain what service will be using the connectivity and why it is being used.	text
TCP/989 FTP-S Data Channel Active Mode	#1	Is this for a FTP-S Implicit Mode transmission ?	yes
			no
	#2	If not for FTP-S describe the usage.	text
TCP/990 FTP- Control Channel	#1	Is this for FTP-S?	yes
			no
	#2	If used for FTP-S Passive Mode - define the data channels to be configured. If for Other - Describe the usage.	text
TCP/992 Telnet over TLS/SSL	#1	Describe the control environment at Citigroup destination system and the containment strategy to keep permitted access to the destination servers or within the approved network segments, by selecting all that apply:	Secured by OS
			zLinux
			zVM
			AS/400
			zVSE
			MVS
			OS/390
			other
	#2	If selecting <u>Other</u>, explain the connectivity	Text
TCP/UDP 995 POP3s	#1	Is this for POP Protocol?	Yes
			No
	#2	If No, What service will be using the port?	text
UDP/1434 MS SQL Server	#1	MS SQL monitor can be used for malicious code, Explain the service utilizing the connectivity and why this is needed.	text

TCP/1494 Citrix - TPA	#1	All network segments are registered TPA segments secured with Appsense and a proxy Whitelist	Attestation
TCP/1494 Citrix - NON TPA	#1	Describe the control environment at Citigroup destination system and the containment strategy to keep permitted access to the destination servers or within the approved network segments	Published application
			Published desktop
	#2	If Desktop, Explain the containment strategy to keep permitted access to the destination servers	text
	#3	Explain why the TPA (Third Party Architecture) environment is not utilized	text
UDP/1604 Citrix	#1	Describe the control environment at Citigroup destination system and the containment strategy to keep permitted access to the destination servers or within the approved network segments	Published application
			Published desktop
	#2	If Desktop, Explain the containment strategy to keep permitted access to the destination servers	text
	#3	Explain why the TPA (Third Party Architecture) environment is not utilized	text
TCP/UDP 2390 RSMTP	#1	All SMTP servers listed in the request are managed by Citi Global Messaging?	Yes
			No
TCP/ 2598 Citrix - TPA	#1	All network segments are registered TPA segments secured with Appsense and a proxy Whitelist	Attestation
TCP/2589 Citrix - NON- TPA	#1	Describe the control environment at Citigroup	Published application

		destination system and the containment strategy to keep permitted access to the destination servers or within the approved network segments	Published desktop	
	#2	If Desktop, Explain the containment strategy to keep permitted access to the destination servers	text	
	#3	Explain why the TPA (Third Party Architecture) environment is not utilized	text	
TCP/3410 Citrix	#1	Describe the control environment at Citigroup destination system and	Published application	
		the containment strategy to keep permitted access to the destination servers or within the approved network segments	Published desktop	
	#2	If Desktop, Explain the containment strategy to keep permitted access to the destination servers	text	
	#3	Explain why the TPA (Third Party Architecture) environment is not utilized	text	
TCP/6000-6063 XTerm/Xwindows	#1	Explain the service utilizing the connectivity and why it is using the TCP_6000-6063:	text	
TCP/7744 Riverbed Tunnel	#1	Is this connectivity traversing the Citi perimeter terminating on a Riverbed device?	Yes	
TCP/7800 Riverbed Tunnel			No	
TCP/7801 Riverbed Tunnel				
TCP/7810 Riverbed Tunnel	#2	Explain the application traffic flow utilizing the connectivity	text	
TCP/7820 Riverbed Tunnel				
TCP/7850 Riverbed Tunnel				
TCP/7860 Riverbed Tunnel				
TCP/7870 Riverbed Tunnel				
TCP/8080 HTTP (proxy)	#1	Is this for Procy Protocol?	Yes	
			No	

	#2	If No, What service will be using the port?	text
TCP/45000 Citrix	#1	Describe the control environment at Citigroup destination system and the containment strategy to keep permitted access to the destination servers or within the approved network segments	Published application
			Published desktop
	#2	If Desktop, Explain the containment strategy to keep permitted access to the destination servers	text
	#3	Explain why the TPA (Third Party Architecture) environment is not utilized	text
IPSEC **Protocol Suite for IPSec Tunnel**	#1	Is the connectivity approved IP peer pairs terminating on a Citi perimeter	Yes
			No
	#2	If No, this deviates from the Network Security Standards. Please explain:	text
GRE **Router-to-Router Tunnel**	#1	Is the connectivity approved IP peer pairs terminating on a Citi perimeter	Yes
			No
	#2	If No, this deviates from the Network Security Standards. Please explain:	text