CVS Health®

External Connections Project

June 2025

Crowe

Table of Contents

I. Project Scope, Deliverables, and Approach 3

II. Executive Summary 4

III. Inventory Overview 5

IV. Inventory Remediation 6

V. Observations & Recommendations (By Connection) 7

Appendix

I. Stakeholder Team Structure 18

Project Scope, Deliverables, and Approach

As part of CVS Health's External Connection Management Governance initiative, Crowe was selected to assist in the consolidation of existing, individual connection inventories into a single, unified external connection inventory over a three-week period. Where inventory information for a specific connection type is incomplete, Crowe has developed a methodology to obtain the missing information and calculated an estimated level of effort required to complete the inventory. The connection types in-scope for the program are detailed below.

In-scope:

- **Secure Managed File Transfer**
  - Secure File Transfer Protocol (SFTP)
  - Sterling File Gateway
- **Collaboration**
  - Microsoft 365
  - eShare
  - Slack
- **Secure Connectivity**
  - Firewall Modifications
  - Business-to-Business Virtual Private Network (B2B VPN)
  - MPLS
- **Virtual Machines**
  - Citrix VMWare
- **APIs & Integration**
  - APIs
  - Application Integrations

Out-of-scope:

- **Secure Managed File Transfer**
  - SSL VPN (Endpoint) – All relevant connections come from CVS-owned devices

Crowe's Approach

1. Crowe held workshops with CVS Health stakeholders, validating the scope and approach of the project.
2. Crowe held interview sessions with CVS Health connection owners and others involved in the management of the connection type, validating the completeness and quality of the inventory, identifying pain points, etc.
3. Crowe began consolidating individual inventories into a single, master-inventory with ECMG required fields. For many connection types, the identification of incomplete inventory reports resulted in a re-prioritization of efforts to document a gap analysis and defined roadmap to completion.
4. Crowe documented action plans and instructional documentation to guide CVS Health through the manual efforts required to complete their external connections inventory.

Deliverables

1. External Connections Report (this document) detailing the current state of CVS Health's individual inventories, the quality of data within, and estimated effort to complete the inventory.
2. ECMG Requirements Document which includes field-by-field instructions for: **a)** Mapping individual inventories to the ECMG mandatory fields, and **b)** Obtaining missing data for each inventory line item for each connection type.
3. ECMG External Connections Inventory – prior to manual data gathering.

Executive Summary

ECMG Initiative Timeline

June 9-14 – Crowe Team was provisioned CVS Health access
June 17-21 – Stakeholder interviews held
June 23-27 – Completed interviews, draft deliverables

Key Takeaways:

1. CVS Health has significant gaps in their SFTP inventory, one of the top-priority connection types for this project.
2. Manual completion of SharePoint, Virtual Machine, and Application Integration inventories may require an excess 3,000 hours of effort each *(note that additional data or automation capabilities may reduce this estimate)*. Estimated effort cannot be calculated for several connection types due to incomplete inventories. See Inventory Correction Heatmap for more details.
3. Several inventories are manually-maintained, which indicates that connections may exist which are not documented in the inventory.

Limitations:

- The timeframe of this project was limited to June 9th – June 30th.
- Several distinct teams and systems were identified over the course of this effort which were NOT previously identified as stakeholders, and it is reasonable to expect that select stakeholders were not interviewed.
- Given limited CVS Health system access, there were cases where select system inventories had not been obtained before the conclusion of the project.

Inventory Overview

Connection Type	Completeness of Inventory	Data Quality by Record	Effort Required to Complete Inventory
Secure File Transfer Protocol (SFTP)	INCOMPLETE	MODERATE	LARGE
Sterling File Gateway	COMPLETE	INVENTORY NOT RECEIVED*	INVENTORY NOT RECEIVED*
Microsoft 365	COMPLETE	POOR	LARGE
Microsoft eShare	COMPLETE	HIGH	MEDIUM
Slack	COMPLETE	MODERATE	MEDIUM
Firewall Rule Modifications	See SFTP, B2B VPN & MPLS		
Business-to-Business Virtual Private Network (B2B VPN)	MANUALLY MAINTAINED	MODERATE	SMALL
MPLS	MANUALLY MAINTAINED	MODERATE	SMALL
Citrix VMWare Virtual Machines	COMPLETE	MODERATE	LARGE
APIs	COMPLETE	INVENTORY NOT RECEIVED*	INVENTORY NOT RECEIVED*
Application Integrations	COMPLETE	INVENTORY NOT RECEIVED*	LARGE

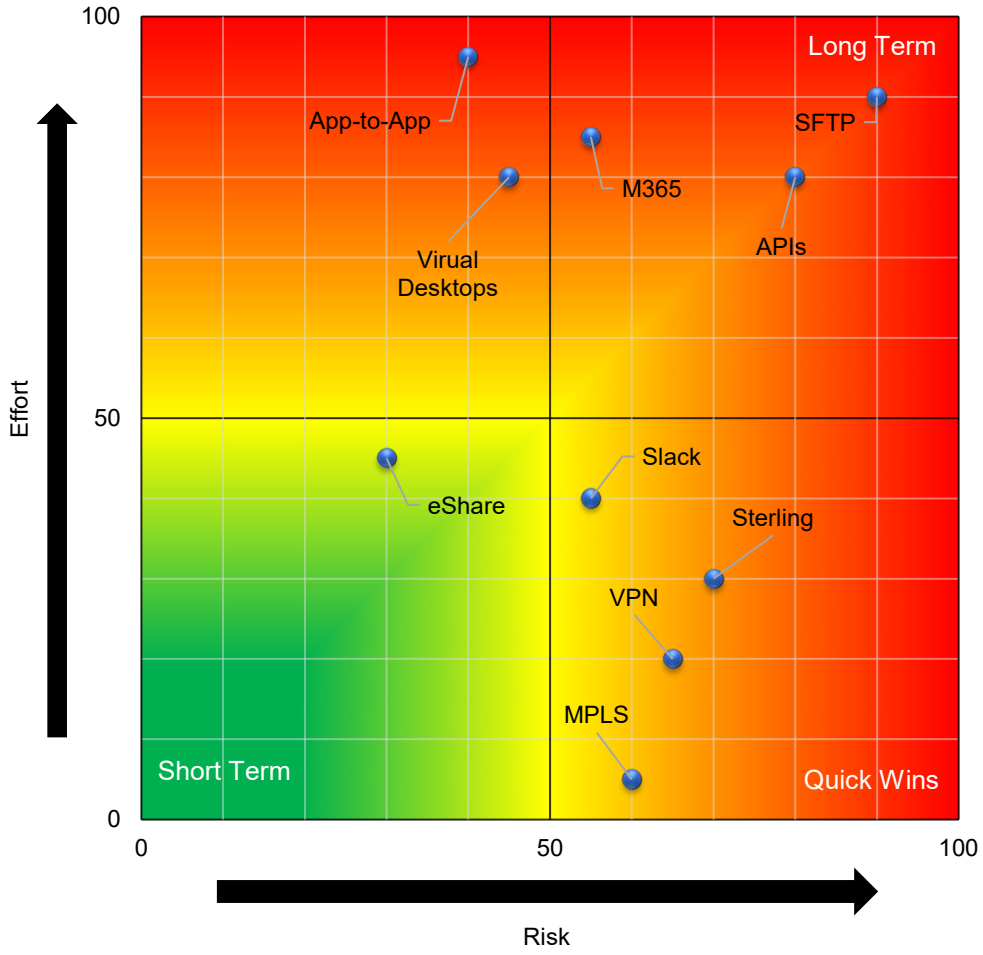
Completeness: *Complete inventories have system-generated inventories readily available. Incomplete inventories are currently known to be incomplete as verified by interviewees. Manually maintained inventories are believed to be complete, but cannot be validated without a system generated list.*

Data Quality: *Average completeness of each record in the inventory. There are 23 mandatory fields in the ECMG requirements.*

Effort: *Estimated effort required by CVS Health to complete the inventory for each connection type (considering both completeness of inventory and any efforts required to manually source missing field information).*

** **Inventory Not Received** indicates that either updated inventory data (potentially with expanded fields) is available but has not yet been received by the SCMG team. As such data quality and effort estimates cannot be confirmed.*

Inventory Remediation



Effort Required in Hours:

Connection Type		Effort
Secure File Transfer Protocol (SFTP)	**N/A**	N/A
Sterling File Gateway	**TBD**	(3-5 Minutes per Record) * (**TBD** Records in Inventory)
Microsoft 365	**3,000 Hours**	(3-5 Minutes per Record) * (**50,000+** Records in Inventory)
Microsoft eShare	**TBD**	(3-5 Minutes per Record) * (**TBD** Records in Inventory)
Slack	**14 Hours**	(3-5 Minutes per Record) * (250 Records in Inventory)
Firewall Rule Modifications	**N/A**	N/A
B2B VPN	**16 Hours**	(2 Minutes per Record) * (500 Records in Inventory)
MPLS	**2.5 Hours**	(2 Minutes per Record) * (70 Records in Inventory)
Citrix VMWare Virtual Machines	**3,000 Hours**	(3-5 Minutes per Record) * (50,000 Records in Inventory)
APIs	**TBD**	(3-5 Minutes per Record) * (**TBD** Records in Inventory)
Application Integrations	**TBD**	(**TBD** Minutes per Record) * (125,000 Records in Inventory)

Secure Managed File Transfer

Secure File Transfer Protocol (SFTP)

Priority 1

Completeness of Inventory	Data Quality by Record	Effort Required
INCOMPLETE	MODERATE	LARGE

Observation	Recommendation
There is no single inventory of CVS Health SFTP connections. Across the enterprise, there are several legacy managed file transfer (MFT) solutions, inventoried and not-inventoried, which support CVS Health's various business units. A majority of these connections are supported by Axway Secure Transport, an MFT solution managed by an Aetna business unit, SFTP Engineering. This team generated a list of SFTP connections which was provided to the ECMG team for review. There is a separate legacy solution also leveraged by a CVS Pharmacy Benefit Management (PBM business unit) SFTP team, as well as several other known solutions, custom and commercial, which support various other CVS business units. Upon inquiry with Frans Westerhof, Lead Director – Software Development/Engineering, it was noted that use of a specific MFT is not currently mandated across the enterprise, however, a new enterprise SFTP solution and request process is currently under development. The ECMG team also met with the File Transfer Implementation (FTI) team, however, this function simply creates new connections and has no inventory. New SFTP connections do not necessarily correspond with a firewall rule change. SFTP Engineering teams can create new connections in pre-approved IP ranges for SFTP use, which may be leveraged depending on the needs of the external party.	CVS should prioritize the completion of the development of their new, centralized SFTP technology and process, and perform the following reconciliatory activities to align legacy SFTP activity with the new process: 1. Initiate a survey across CVS Health companies, business units, and other operating groups to identify the MFT solution supporting their function. For all groups deviating from the enterprise process, an action plan for migration should be determined. 2. Perform reconciliatory firewall log reviews to identify SFTP activity occurring outside of new processes.

** See a description of all personnel interviewed in Appendix I.*

Secure Managed File Transfer

Sterling File Gateway

Priority 1

Completeness of Inventory	Data Quality by Record	Effort Required
COMPLETE	INVENTORY NOT RECEIVED	INVENTORY NOT RECEIVED

Observation	Recommendation
At the time of this project, the ECMG team has not received any inventory of Sterling File Gateway connections. There are no concerns that the inventory may be incomplete given stakeholders generate the connection inventory directly within the Sterling File Gateway solution. The ECMG team has received commitment from Juliano El Aaraj, Software Development Engineer, that an inventory will be provided by July 7th, 2025. * * * A new Sterling File Gateway connection requires a request submitted via the Sterling Business Integrator (STIBO), a master data management solution used to onboard new connection. STIBO requests often include business-level information which can be used to determine engagement info and potentially other ECMG mandatory fields. Following onboarding of the external party in STIBO, Sterling File Gateway is used to create a connection and schedule / manage file transfers.	Following receipt of a Sterling File Gateway inventory, develop field-by-field instructions for manually compiling this information similar to those documented in the ECMG Requirements Document. Calculate the estimated number of hours required to manually obtain the necessary information to populate the remaining ECMG mandatory fields for all records of this connection type. Prioritize completion of the inventory as needed.

** See a description of all personnel interviewed in Appendix I.*

Collaboration

Microsoft 365

Priority 1

Completeness of Inventory	Data Quality by Record	Effort Required
COMPLETE	POOR	LARGE

Observation	Recommendation
CVS Health currently uses AvePoint to manage the external sharing of Microsoft 365 content including SharePoint / SharePoint Online, Microsoft Teams, and OneDrive content. Refreshed inventory information is available on demand within AvePoint. Following inquiry with Laura Shepherd, Staff Security Engineer, the ECMG team must request access to AvePoint to review and export in-scope data. The inventory is complete given its system-generated nature and integration with CVS Health M365 tenants. **Note:** eShare is a solution with underlying infrastructure supported by OneDrive and SharePoint, however, it is segmented from other externally shared M365 content.	There are currently over 16,000 external SharePoint connections, with minimal SharePoint Online and Microsoft Teams connections. ECMG must obtain access to AvePoint before further determining the extent of the data within, however, the data includes at least the external entity name, as well as internal (CVS Health) and external membership. See field-by-field instructions for manually compiling remaining ECMG required fields in the ECMG Requirements Document. Calculate the estimated number of hours required to manually obtain the necessary information to populate the remaining ECMG mandatory fields for all records of this connection type. Prioritize completion of the inventory as needed.

** See a description of all personnel interviewed in Appendix I.*

Collaboration

Microsoft eShare

Priority 1

Completeness of Inventory	Data Quality by Record	Effort Required
COMPLETE	HIGH	MEDIUM

Observation	Recommendation
CVS Health has a complete inventory of their Microsoft eShare 'Shares', available for review in a PowerBI dashboard, which gives Laura Shepherd, Information Security, insight into all active Shares, and current external recipients. Given that CVS Health Information Security is capable of producing system-generated reports of connections, the ECMG team is comfortable that the inventory will be complete when provided. This report has not been provided to date. However, per inquiry this report should be built in early July 2025 by a member of Laura Shepherd's team.	The current inventory available contains sufficient information to leverage other CVS Health resources (primarily ProcessUnity) to obtain information for all other ECMG mandatory data fields. See field-by-field instructions for manually compiling this information in the ECMG Requirements Document. Calculate the estimated number of hours required to manually obtain the necessary information to populate the remaining ECMG mandatory fields for all records of this connection type. Prioritize completion of the inventory as needed.

** See a description of all personnel interviewed in Appendix I.*

Collaboration

Slack

Priority 1

Completeness of Inventory	Data Quality by Record	Effort Required
COMPLETE	MODERATE	MEDIUM

Observation	Recommendation
At the time of this project, the ECMG team has not received a complete inventory of Slack connections. A report detailing all Slack connections, with user-level external party membership, is currently being obtained by Brandon Tarr, Sr. Compute Engineer. There is no estimated timeframe for this inventory being provided, as emails to Brandon from Dino Dotenoglou on June 19th and June 25th have not received a response. The ECMG team has a partially-complete list of Slack connections and was identified as incomplete during a screensharing session with Slack stakeholders on June 17, 2025. During this screensharing session, it was noted that CVS Health has insight into all Slack connections, including relevant connection owners (internal) and members (external) which can be accessed on demand within Slack.	Following receipt of a Slack inventory, validate that the field-by-field instructions for manually compiling remaining data for mandatory fields documented in the ECMG Requirements Document. Calculate the estimated number of hours required to manually obtain the necessary information to populate the remaining ECMG mandatory fields for all records of this connection type. Prioritize completion of the inventory as needed.

** See a description of all personnel interviewed in Appendix I.*

Firewall Rule Modifications

Priority 1

Completeness of Inventory	Data Quality by Record	Effort Required
See SFTP, B2B VPN, & MPLS		

Observation	Recommendation
The ECMG team interviewed several personnel from the Firewall Operations and Firewall Project Management functions as their roles support the enablement and/or management of relevant B2B VPN, MPLS, and SFTP connections, and noted the following: • **SFTP** – Firewall Operations is not inherently involved in the SFTP setup process. CVS Health has designated IP ranges for SFTP use. As such, Firewall Operations will only address tickets which require SFTP use outside these pre-approved ranges. • **B2B VPN -** Similarly to SFTP, Firewall Operations addresses tickets involving VPN connections within SNOW, as they are received. Per inquiry, many legacy connections exist with limited documentation. There is currently a firewall update project underway which involves identifying owners for legacy connections, validating if the connection is still needed, and modifying connections to support the services still required. • **MPLS** – Changes in MPLS connections are rare, and while new requests have an associated RITM ticket, legacy connections may not be sufficiently documented.	See individual connection types for further recommendations: • SFTP • B2B VPN • MPLS

** See a description of all personnel interviewed in Appendix I.*

Secure Connectivity

B2B Virtual Private Network

Priority 1

Completeness of Inventory	Data Quality by Record	Effort Required
MANUALLY MAINTAINED	MODERATE	SMALL

Observation	Recommendation
B2B VPN connection inventories are documented in segmented inventories organized by originating data center. Aetna VPN connections from the Middletown and Windsor data centers are tracked separately in manually maintained spreadsheets. There are approximately 200 total connections documented (active and inactive). CVS VPN connections from the Rhode Island and Arizona data centers are tracked in a manually maintained spreadsheet, following a migration activity which was performed in 2024. There are approximately 350 total VPN connections documented (active and inactive). Given the manual nature of these inventories, it is possible undocumented connections exist. There are limited external parties with no internal or external contact information.	See field-by-field instructions for manually compiling this information in the ECMG Requirements Document. An estimated effort of **16 hours** (2 Minutes per Record) * (500 Records in Inventory) is required for a resource to manually obtain the information to fill the remaining mandatory fields for each incomplete record in the inventory. In-scope systems to be used to obtain this information include • ServiceNow • ProcessUnity

** See a description of all personnel interviewed in Appendix I.*

Secure Connectivity

MPLS

Priority 1

Completeness of Inventory	Data Quality by Record	Effort Required
MANUALLY MAINTAINED	MODERATE	SMALL

Observation	Recommendation
MPLS connection inventories are documented in segmented inventories organized by originating data center. Aetna MPLS connections from the Middletown and Windsor data centers are tracked separately in manually maintained spreadsheets. There are under 30 total MPLS connections with these Aetna data centers and external parties. CVS MPLS connections from the Rhode Island and Arizona data centers are tracked in a manually maintained spreadsheet, following a migration activity which was performed in 2024. There are under 40 total MPLS connections with these CVS data centers and external parties. Given the manual nature of these inventories, it is possible undocumented MPLS connections exist. There are limited external parties with no internal or external contact information.	Given the relatively low number of active connections, a manual effort to obtain the remaining data is feasible. See field-by-field instructions for manually compiling this information in the ECMG Requirements Document. An estimated effort of **2.5 hours** (2 Minutes per Record) * (70 Records in Inventory) is required for a resource to manually obtain the information to fill the remaining mandatory fields for each incomplete record in the inventory. In-scope systems to be used to obtain this information include: • ServiceNow • ProcessUnity

** See a description of all personnel interviewed in Appendix I.*

Virtual Machines

Citrix VMWare Virtual Machines

Priority 1

Completeness of Inventory	Data Quality by Record	Effort Required
COMPLETE	MODERATE	LARGE

Observation	Recommendation
The ECMG team met with Compute / Engineering personnel involved in the management of Citrix VMWare Virtual Machines. This team can export a listing of virtual machines, their device name, and associated end-user. However, many VMs support external workers, and as such this inventory does not allow the ECMG team to map the VM inventory to an entity (e.g. end-user's primary employer). As such, the ECMG team also met with stakeholders of the Colleague Experience Engineering function, which uses several distinct solutions to facilitate onboarding, including Excalibur, Glide, and Eternity. Per inquiry, these systems should allow the ECMG insight into all external workers' employing organization. **At this time, no Excalibur, Glide, or Eternity has been available to the ECMG team for review.**	Following receipt of Excalibur, Glide, and Eternity data, virtual machines from the inventory provided should be analyzed to map each external worker's employing organization. For internally-owned VMs, these machines may be marked out of scope. For remaining VMs, first map each line item to an external entity. **After** determining the external entity's name, see field-by-field instructions for manually compiling this information in the ECMG Requirements Document. Lastly, calculate the estimated effort in **number of hours** (e.g (2 Minutes per Record) * (70 Records in Inventory)) for a resource to manually obtain the information to fill the remaining mandatory fields for each incomplete record in the inventory. **Given the number of records in preliminary inventory reviews, the effort may exceed 3,000 hours.** In-scope systems to be used to obtain this information include: • ServiceNow • ProcessUnity

** See a description of all personnel interviewed in Appendix I.*

API & Integration

APIs

Priority 1

Completeness of Inventory	Data Quality by Record	Effort Required
COMPLETE	INVENTORY NOT RECEIVED	INVENTORY NOT RECEIVED

Observation	Recommendation
At the time of this engagement, limited information related to APIs was available and provided. A document was provided which appears to be a system-generated listing which would provide comfort that the inventory is complete, however, the report is missing too many ECMG required fields to develop a methodology to complete each inventory record. A meeting is scheduled with API Engineering stakeholders for July 2, 2025.	Following receipt of an inventory, develop field-by-field instructions for manually compiling this information similar to those documented in the ECMG Requirements Document. Calculate the estimated number of hours required to manually obtain the necessary information to populate the remaining ECMG mandatory fields for all records of this connection type. Prioritize completion of the inventory as needed.

Application Integration

Priority 1

Completeness of Inventory	Data Quality by Record	Effort Required
COMPLETE	INVENTORY NOT RECEIVED	LARGE

Observation	Recommendation
CVS Health currently has an effort underway to develop an inventory of all application-to-application connections (e.g. extensions). Per inquiry with Victoria Garstka, Sr. Security Engineer, Identity Management, these integrations are documented in managed via two applications: • AppOmni – SaaS-to-SaaS integrations, 115,000 records • Zscaler – Cloud-based applications, 8,000 records Given that both solutions are capable of producing system-generated reports of connections, the ECMG team is comfortable that the inventory is complete.	Following receipt of an inventory, develop field-by-field instructions for manually compiling this information similar to those documented in the ECMG Requirements Document. Calculate the estimated number of hours required to manually obtain the necessary information to populate the remaining ECMG mandatory fields for all records of this connection type. Prioritize completion of the inventory as needed.

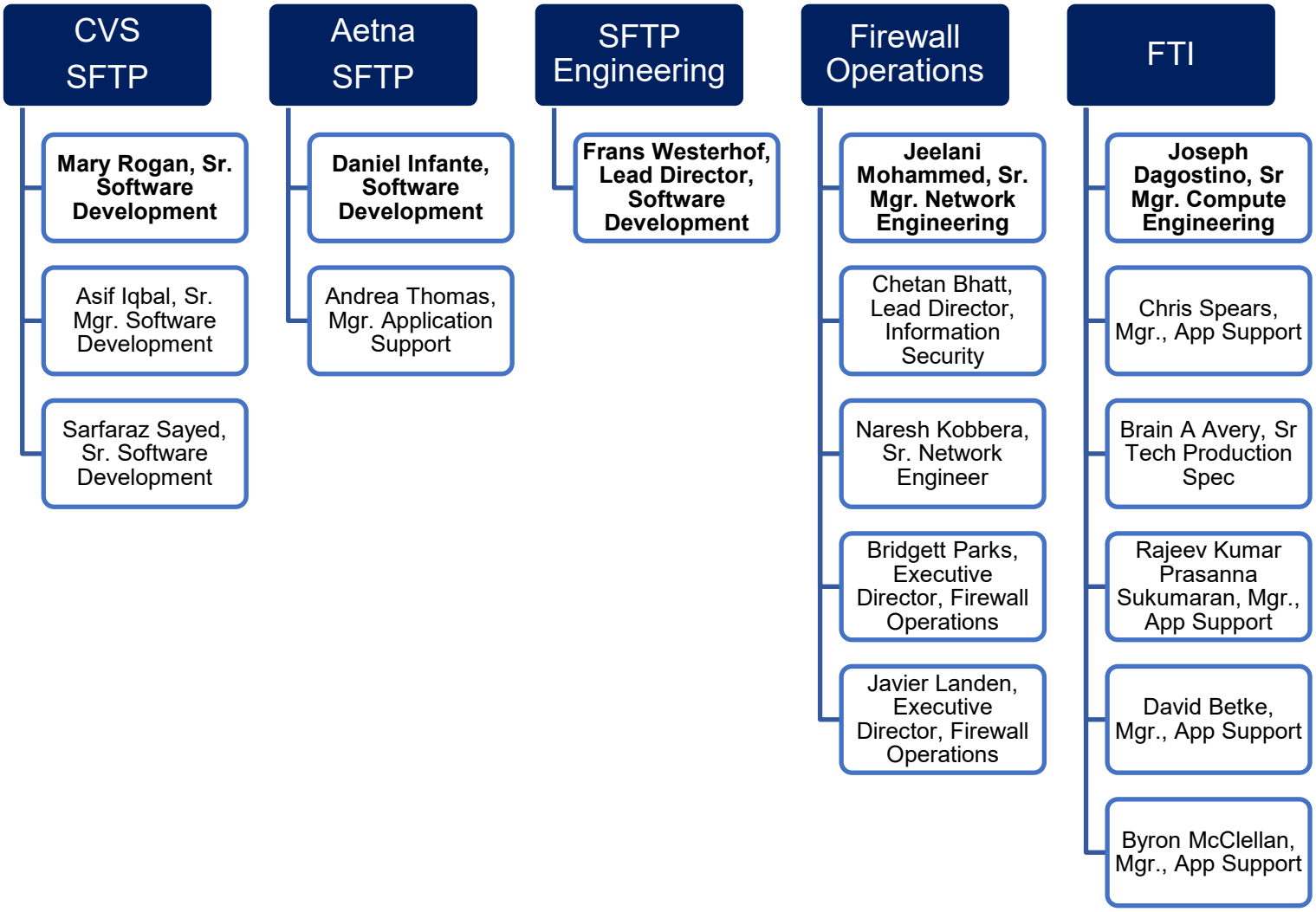
** See a description of all personnel interviewed in Appendix I.*

Appendix I

Connection Stakeholders

Primary point-of-contact(s) bolded.

Secure File Transfer Protocol (SFTP)

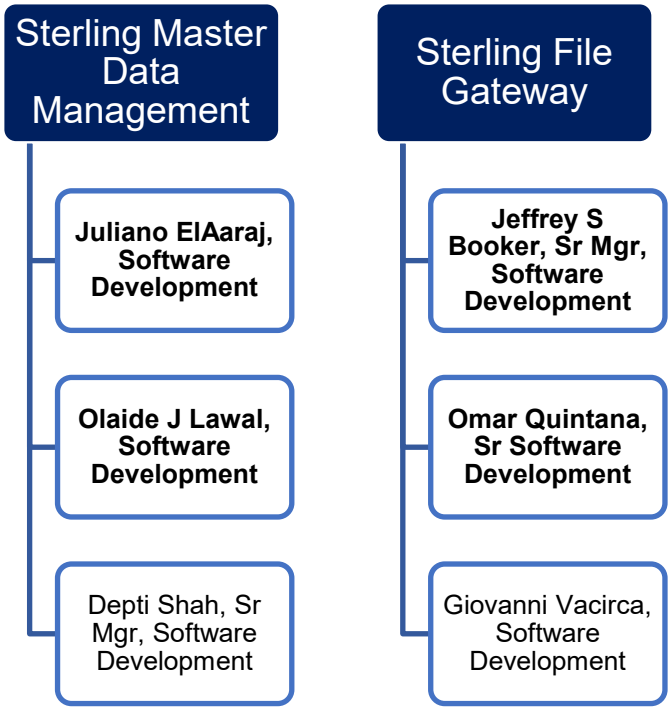


Appendix I

Connection Stakeholders

Primary point-of-contact(s) bolded.

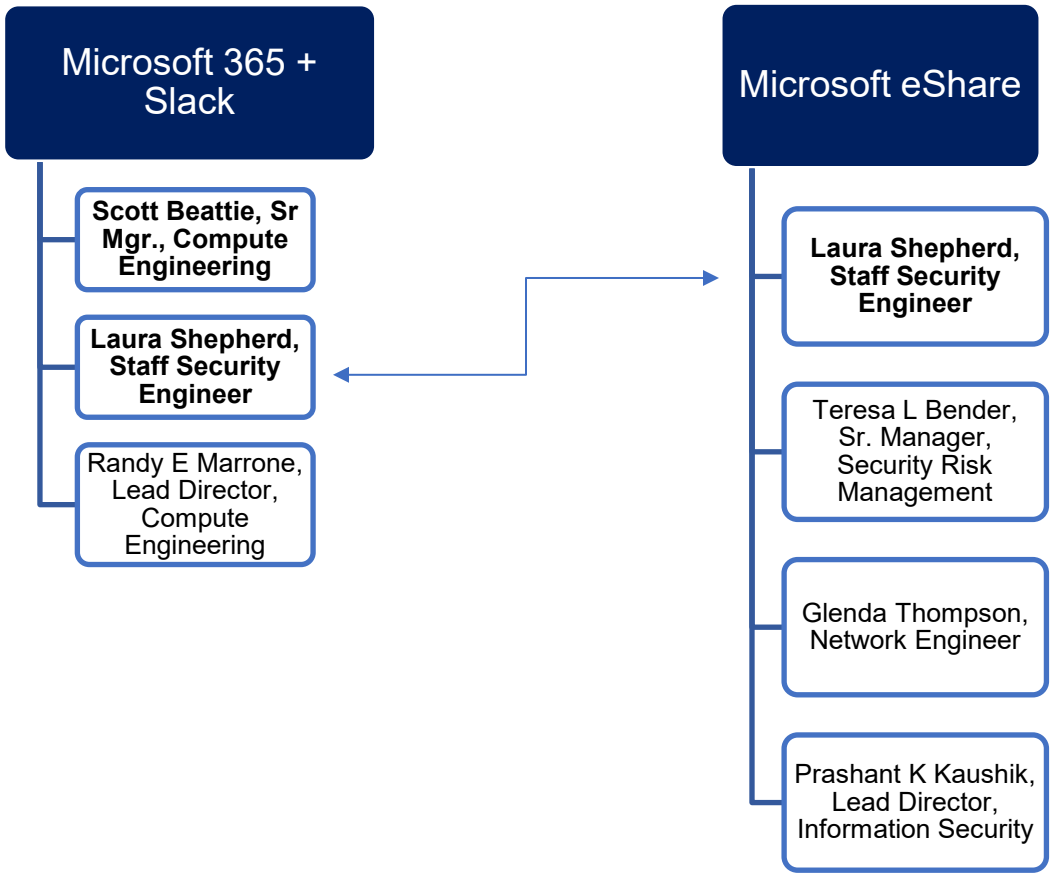
Sterling File Gateway



Appendix I

Connection Stakeholders

Primary point-of-contact(s) bolded.

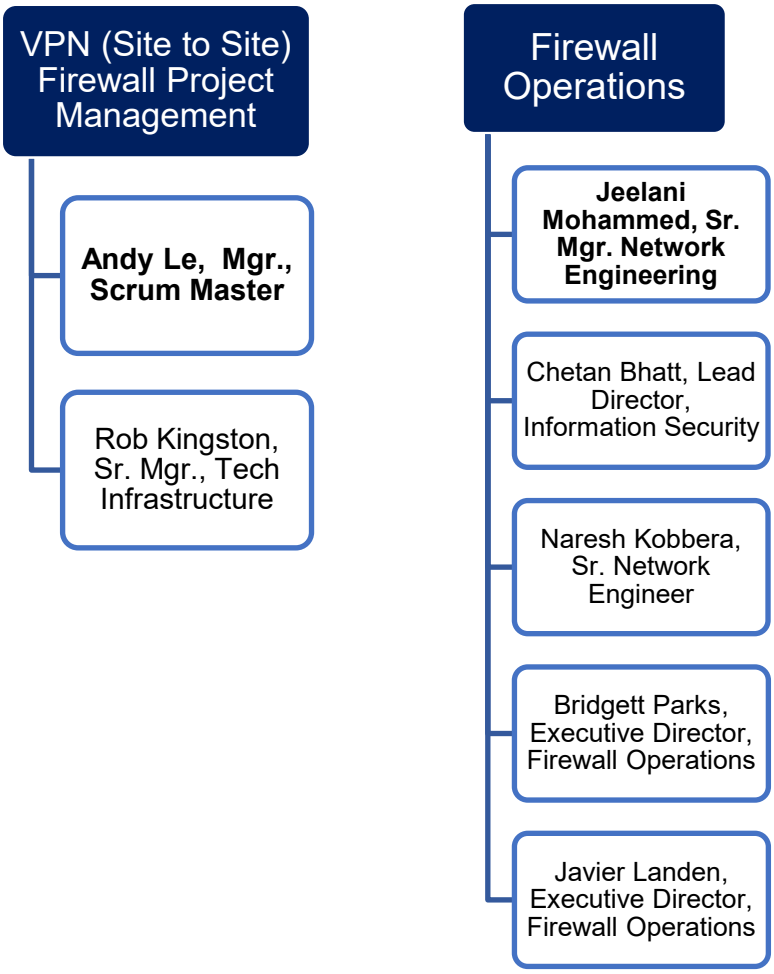


Appendix I

Connection Stakeholders

Primary point-of-contact(s) bolded.

Firewall / VPN / MPLS

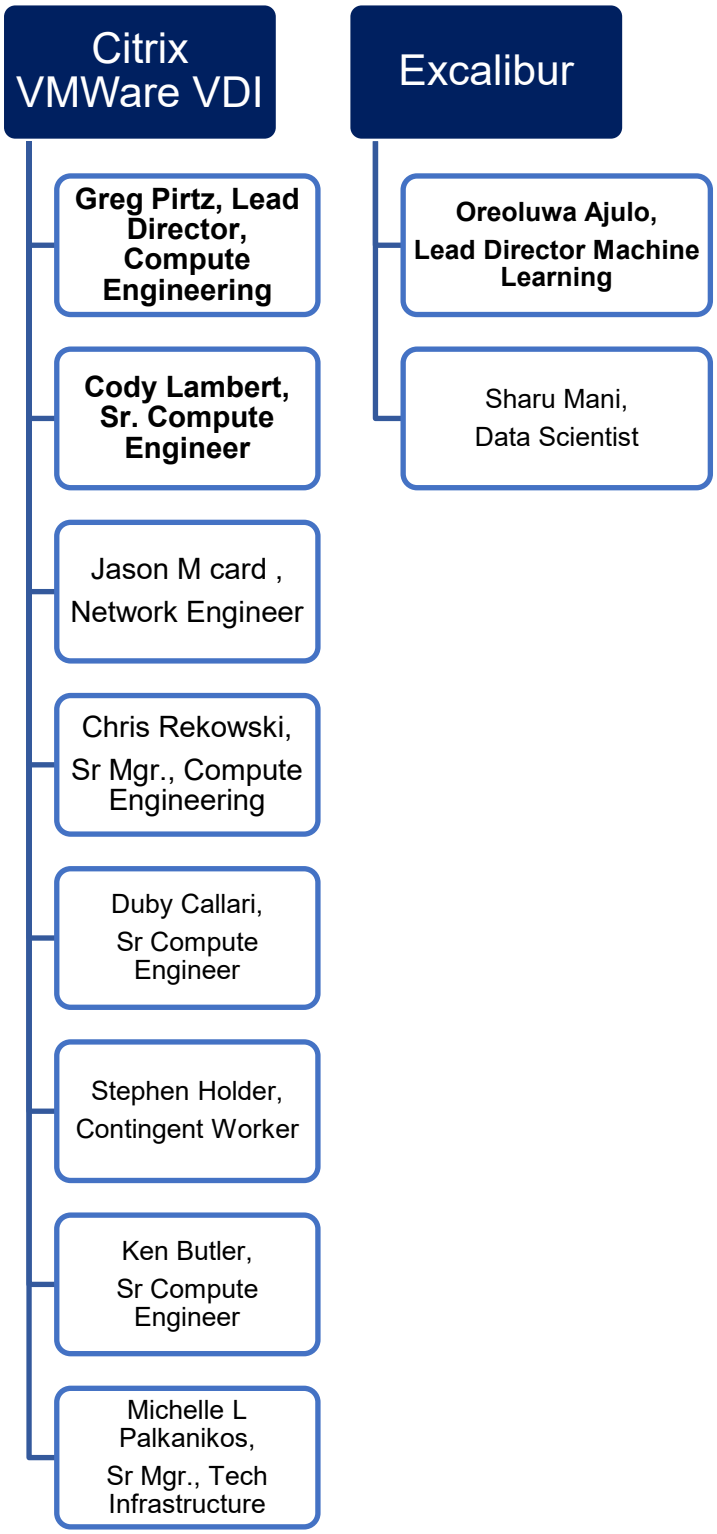


Appendix I

Connection Stakeholders

Primary point-of-contact(s) bolded.

Citrix VMWare



Appendix I

Connection Stakeholders

Primary point-of-contact(s) bolded.

APIs & App-to-App

API Engineering

- Giuseppe Pellegrino, Lead Architect
- Roy Klein, Principal Software Development Engineer
- Pawan K Agrawal, Sr Mgr., Software Development Engineering
- Rinu G Dhanaraj, Staff Software Development Engineer
- Yanay Ibanez, Sr Mgr, Software Development Engineering

API Engineering (cont.)

- Jeevesh Kumar, Sr. Mgr., Software Development Engineering
- Puneet Poddar, Lead Director, Software Development Engineering
- Imad Belabbes, Lead Director, Staff Software Development Engineering
- Chad Mason, Lead Director, Software Development Engineering

API Security

- **Christopher Kwabi, Executive Director, Software Development**
- Colleen Glasgow, Executive Director, Information Security
- Rosemary Burns, Lead Director, Information Security

App-to-App Connections

- **Victoria L Garstka, Sr Security Engineer**
- Carl J Cousino, Sr Mgr, Info Security

Cyber Expertise with patient safety in mind

Retail Pharmacy | Healthcare | Pharmaceutical

Strategy

Governance, Compliance and Reporting

Cyber Program Design & Roadmaps
Align your cyber program with business strategy; establish a roadmap to continue driving patient safety and resiliency

Policies & Procedures
Establish policies and procedures that your employees, suppliers and contractors will understand

Audit & Control Frameworks
Map your cyber audit and control framework for OCR audit readiness and other application laws and regulations

Board and C-Suite Reporting
Report on cyber risk through KRI's and economics in a way that business leaders understand

M&A Due Diligence
Enable business growth through streamlined cyber M&A due diligence planning and execution

Compliance Assessments
Perform compliance assessments against HIPAA, HITRUST and other authoritative sources relevant to your business

Protect

Risk Management, Privacy, Tech Enablement

Risk Assessments & Security Remediation
Assess risks for your health applications, IoT devices, cloud, mobile and AI with security remediation experts

Third Party Risk Management
Design a third-party risk framework that streamlines intake, due diligence, and ongoing assessments

Privacy & Data Protection
Design a program with enhanced patient privacy assessments in alignment with global and US privacy laws

Penetration Testing
Identify vulnerabilities that can impact your patient systems and data integrity

Technology Enablement
Implement cyber GRC and privacy systems such as ServiceNow, OneTrust, ProcessUnity, and more

AI Governance & Risk Management
Establish processes and procedures to govern growing AI usage and manage risks to your health organization

Respond

Incident Response, Digital Forensics, Legal and Insurance Support

Business Resiliency
Design a business resiliency program with enhanced business process inventories, BIA's, and BC/DR plans

Incident Response
Respond to ransomware and data breaches with defense against nation states and organized crime

Digital Forensics & Investigations
Identify, collect and preserve data for digital and employee investigations; leverage expert witness testimony

Government & Regulatory Enforcement
Respond to regulatory inquiries, actions, and consent orders with appropriate remediation activities

Electronic Discovery & Litigation Intelligence
Map and discover data to enable case analysis and search process support; leverage expert witness testimony

Analysis & Reporting
Analyze and report results to boardroom and executive leadership including economic loss and long-term fallout

There's nothing generic about what we do for our clients.

We know our clients inside and out. We live and breathe it. Our insights, technologies, and solutions are crafted out of the challenges facing organizations like yours today.

Together, we can help the industry manage change and uncertainty. We have over 80 years of experience in banking, bringing value to our clients every day.

Crowe by the numbers

- 5,500+ professionals in the United States
- Dedicated, industry-focused team members.
- Crowe Global network enabling our clients to solve complex challenges around the globe.