NIST SPECIAL PUBLICATION 1800-28B

Data Confidentiality:
Identifying and Protecting Assets Against Data Breaches

Volume B:
Approach, Architecture, and Security Characteristics

William Fisher
National Cybersecurity Center of Excellence
NIST

R. Eugene Craft
Michael Ekstrom
Julian Sexton
John Sweetnam
The MITRE Corporation
McLean, Virginia

February 2024

FINAL

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

FEEDBACK

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at ds-nccoe@nist.gov.

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

Attacks that target data are of concern to companies and organizations across many industries. Data breaches represent a threat that can have monetary, reputational, and legal impacts. This guide seeks to provide guidance concerning the threat of data breaches, exemplifying standards and technologies that are useful for a variety of organizations defending against this threat. Specifically, this guide seeks to help organizations identify and protect assets, including data, against a data confidentiality attack.

KEYWORDS

asset management; cybersecurity framework; data breach; data confidentiality; data protection; identify; malicious actor; malware; protect; ransomware

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Victor Ortiz	PKWARE
Jim Wyne	PKWARE
Steve Petruzzo	Qcor
Billy Stewart	Qcor
Norman Field	StrongKey
Patrick Leung	StrongKey
Arshad Noor	StrongKey
Lauren Acierto	The MITRE Corporation
Spike Dog	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Brian Johnson	The MITRE Corporation
Lauren Lusty	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Julie Snyder	The MITRE Corporation
Lauren Swan	The MITRE Corporation
Anne Townsend	The MITRE Corporation
Jessica Walton	The MITRE Corporation

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product

components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Avrio Software (now known as Aer-stone)	Avrio SIFT
Cisco Systems	Duo
Dispel	Dispel
FireEye	FireEye Helix
Qcor	Qcor ForceField
PKWARE	PKWARE PKProtect
StrongKey	StrongKey Tellaro
Symantec, a Division of Broadcom	Symantec Web Isolation

DOCUMENT CONVENTIONS

The terms "shall" and "shall not" indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms "should" and "should not" indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms "may" and "need not" indicate a course of action permissible within the limits of the publication. The terms "can" and "cannot" indicate a possibility and capability, whether material, physical, or causal.

PATENT DISCLOSURE NOTICE

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Contents

List of Figures

List of Tables

1 Summary

In our data-driven world, organizations must prioritize cybersecurity and privacy as part of their business risk management strategy. Specifically, data confidentiality remains a challenge as attacks against an organization's data can compromise emails, employee records, financial records, and customer information—impacting business operations, revenue, and reputation.

Confidentiality is defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information"[1]. Data confidentiality makes sure that only authorized users can access data and use it in an authorized manner. Ensuring data confidentiality should be a priority for any organization regardless of industry. A loss of data confidentiality can be of great impact to not just the company or organization, but also to the individuals who have trusted the organization with their data.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) developed an example solution to address data security and privacy needs. This project fits within a larger series of Data Security projects that are organized by the elements of the Confidentiality, Integrity, Availability (CIA) triad, and the NIST Cybersecurity Framework's (CSF) Core Functions: Identify, Protect, Detect, Respond, and Recover.

> **Note:** This project was initiated before the release of the DRAFT NIST CSF 2.0 and thus does not include the newly added GOVERN function. The DRAFT NIST CSF 2.0 defines Govern as "Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy". The govern function cuts across the other CSF functions. Though this document focuses on technical capabilities, it's intended that those capabilities would support an organizational governance function in managing data confidentiality attack risk.

Figure 1-1 Data Security Project Mapping

Cybersecurity Framework Functions	Information Security Goals		
	Confidentiality	Integrity	Availability
Identify	1800-28 (you are here)	1800-25	
Protect			
Detect	1800-29	1800-26	
Respond			
Recover		1800-11	

The goals of this NIST Cybersecurity Practice Guide are to assist organizations in identifying and protecting their assets and data in order to prepare for and prevent a data confidentiality event. This guide will help organizations:

- Inventory data storage and data flows
- Protect against confidentiality attacks against hosts, the network and enterprise components
- Protect enterprise data at rest, in transit, and in use
- Configure logging and audit capabilities to meet organizational requirements
- Implement access controls to sensitive data
- Implement authentication mechanisms for host and network access
- Enumerate data flows and problematic data actions in line with the NIST Privacy Framework

In addition to the guidance provided in these documents, NIST has many resources available to help organizations to identify and protect data:

- NIST Special Publication 1800-25, Data Integrity: Identifying and Protecting Assets Against Ransomware and other Destructive Events [2]
- NIST Special Publication 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops [5]
- NIST Special Publication 800-46, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security [6]
- NIST Privacy Framework [7]
- NIST Cybersecurity Framework [8]
- NIST Interagency Report 8374, Ransomware Risk Management: A Cybersecurity Framework Profile [9]
- NIST Special Publication 800-160, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach [10]

1.1 Challenge

Data confidentiality is a challenge because all data exists to be accessible by some number of authorized people or systems. Data access can lead to a data breach when access is achieved or given to an unauthorized person or system. Challenges for an organization to maintain data confidential result from the sheer volume of an organization's data, the many ways users can access the data (on-site versus remote, computer versus mobile device), and the potential for the compromise of valid user credentials being used by unauthorized users.

NIST SP 1800-28 focuses on applying the Identify and Protect Functions of the NIST Cybersecurity Framework to address the challenges related to categorizing authorized and unauthorized data access. This document helps organizations address identifying potential breaches of data confidentiality as well as protecting against the resulting losses.

Additional challenges arise when defining what it means to "identify" or "protect" data. In the NCCoE's previous work on Data Integrity (1800-25 [2], 1800-26 [3], and 1800-11 [4]), it was possible to define recovery as a rollback of the compromised data to a point in time before it was altered. With respect to a loss of data confidentiality, there is no such process by which to "undo" the effects of such a loss—

once digital data is in the hands of an unauthorized user, there is no guaranteed method by which to get all copies of the data back. This leaves an organization and the affected individuals with non-technical mitigations for the consequences of the breach (financial, reputational, etc.), as well as the ability of the organization to apply the lessons learned to technical improvements earlier in the timeline to prevent against future breaches.

1.2 Solution

The NCCoE developed this two-part solution to address considerations for both data security and data privacy to help organizations manage the risk of a data confidentiality attack. The work in 1800-29 addresses an organization's actions during and after a loss of data confidentiality (the remaining NIST CSF Functions of Detect, Respond, and Recover) while this guide's focus is on the needs prior to a loss of data confidentiality (by focusing on the NIST CSF Functions Identify and Protect). The solution utilizes commercially available tools to provide relevant capabilities such as automated data sensitivity detection, access controls for data, encryption of potential confidential data, and multifactor authentication, among others.

1.3 Benefits

Organizations can use this guide to help:

- Evaluate their data confidentiality concerns

- Determine if their data security needs align with the data confidentiality challenges identified in this guide

- Conduct a gap analysis to determine the distance between the current state and desired state of the organization's data confidentiality protections

- Perform a feasibility assessment for implementing the protections described in this guide

- Determine a business continuity analysis to identify potential impacts on business operations as a result of a loss of data confidentiality.

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate the data confidentiality capabilities described in this document. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-28A: Executive Summary

- NIST SP 1800-28B: Approach, Architecture, and Security Characteristics – what we built and why (you are here)

- NIST SP 1800-28C: How-To Guides – instructions for building the example solution

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-28A*, which describes the following topics:

- challenges that enterprises face in identifying vulnerable assets and protecting them from data breaches

- example solution built at the NCCoE

- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, *NIST SP 1800-28B*, which describes what we did and why. The following sections will be of particular interest:

- Section 3.5, Risk Assessment, provides a description of the risk analysis we performed

- Section 3.6, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the *Executive Summary, NIST SP 1800-28A*, with your leadership team members to help them understand the importance of adopting standards-based solutions to protecting against losses in data confidentiality.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, *NIST SP 1800-28C*, to replicate all or parts of the build created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a security architecture that protects against data breaches. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, lists the products we used and maps them to the cybersecurity and privacy controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to ds-nccoe@nist.gov.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the NCCoE Style Guide.
Bold	names of menus, options, command buttons, and fields	Choose **File** > **Edit**.
`Monospace`	command-line input, on-screen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
[blue text](#)	link to other parts of the document, a web URL (uniform resource locator), or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

3 Approach

The NCCoE is developing a set of data confidentiality projects mapped to the five Functions of the NIST Cybersecurity Framework Core. This project centers on identifying and protecting vulnerable data from attack. Our commercial collaboration partners have volunteered to provide the products that provide this example solution for the problems raised in each of our use cases. Through this collaboration, our goal is to create actionable recommendations for organizations and individuals trying to solve data confidentiality issues.

3.1 Audience

The architecture of this project and accompanying documentation targets three distinct groups of readers. The first is those personally managing, implementing, installing and configuring IT security solutions for their organization. The walkthroughs of installation and configuration of the chosen commercial products, as well as any of our notes on lessons learned, work to ease the challenge of implementing security best practices. This guide also serves as a starting point for those addressing these security issues for the first time, and a reference for experienced admins who want to do better.

The second group are those tasked with establishing broader security policies for their organizations. Reviewing the threats each organization needs to account for and their potential solutions allows for more robust and efficient security policy to be generated with greater ease.

The final group are those individuals responsible for the legal ramifications of breaches of confidentiality. Many organizations have legal obligations to take steps to proactively protect the personal data or personally identifiable information (PII) of individuals they process. The ramifications

for failing to adequately protect PII can have severe consequences for both individuals and follow on consequences for the organizations as a whole.

This guide will allow potential adopters to assess the feasibility of implementing data confidentiality best practices within the IT systems of their own organization.

3.2 Scope

This document provides guidance on identifying potentially sensitive data and protecting against a loss of data confidentiality. Refer to Figure 1-1 to understand how this document fits within the larger set of NCCoE Data Security projects, as organized by the CIA triad and the functions of the NIST Cybersecurity Framework Core.

3.3 Assumptions

The technical solution developed at the NCCoE and represented in this guide does not incorporate the non-technical aspects of managing the confidentiality of an organization's data. The non-technical components could include (but are not limited to):

- applicable legal requirements based on pertinent jurisdictions
- corporate or other superseding policies relevant to confidentiality and privacy
- standard operating procedures in the event of a loss of data confidentiality
- public relations strategies

This project is guided by the following assumptions:

- The solution was developed in a laboratory environment and is limited in the size and scale of data.
- Only a subset of products relevant to data confidentiality are included in this project, as such organizations should consider the guiding principles of this document when evaluating their organization's needs against the product landscape at the time of their IT implementation.

3.4 Privacy Considerations

Because privacy risks may arise as a result of a loss of confidentiality of data, this guide includes privacy considerations. This section gives a primer for why privacy is important to protect, the relationship between privacy and cybersecurity risk, as well as NIST's approach to privacy risk assessment.

In today's digital landscape, consumers conduct much of their lives on the internet. Data processing, which includes any operations taken with data, including the collection, usage, storage, and sharing of data by organizations, can result in privacy problems for individuals. Privacy risks can evolve with changes in technology and associated data processing. How organizations treat privacy has a direct bearing on their perceived trustworthiness. Recognizing the evolving privacy impacts of technology on individuals, governments across the globe are working to address their concerns through new or updated laws and regulations.

Following an open and transparent development process, NIST published the NIST Privacy Framework, Version 1.0 to help organizations better identify and manage their privacy risks, build trust with customers and partners, and meet their compliance obligations. The Privacy Framework Core provides

privacy outcomes that organizations may wish to achieve as part of a privacy risk management program. The Privacy Framework also discusses privacy engineering objectives that can be used to help organizations prioritize their privacy risk management activities. The privacy engineering objectives are:

- Predictability: Enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system
- Manageability: Providing the capability for granular administration of data, including collection, alteration, deletion, and selective disclosure
- Disassociability: Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system

It is important for individuals and organizations to understand the relationship between cybersecurity and privacy. As noted in Section 1.2.1 of the *NIST Privacy Framework* [8], having a general understanding of the different origins of cybersecurity and privacy risks is important for determining the most effective solutions to address the risks. Figure 3-1 illustrates this relationship, showing that some privacy risks arise from cybersecurity risks, and some are unrelated to cybersecurity risks.

Figure 3-1 Cybersecurity and Privacy Risk Relationship
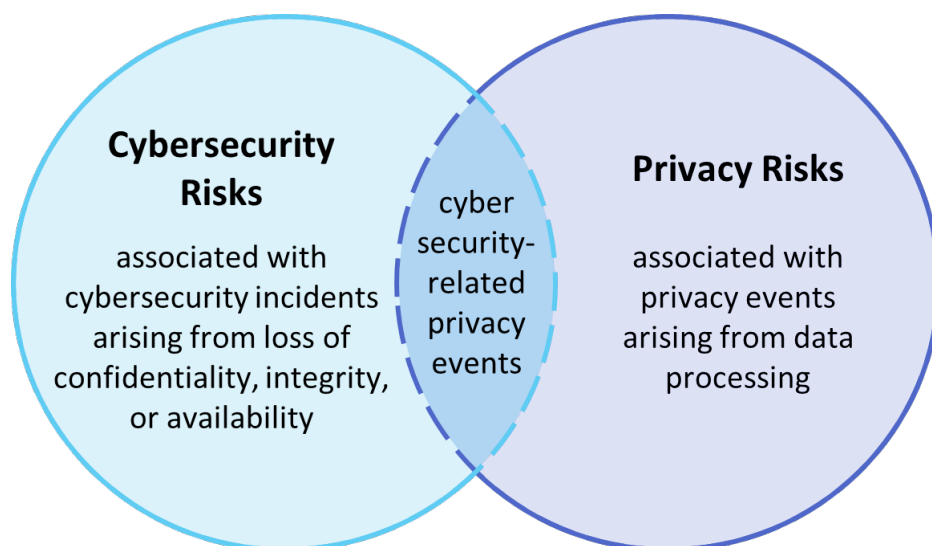
Though a data confidentiality breach may lead to privacy problems for individuals, it is important to note that privacy risks can arise without a cybersecurity incident. For example, an organization might process data in ways that violates an individual's privacy without that data having been breached or compromised through a security incident. This type of issue can occur under a variety of scenarios, such as when data is stored for extended periods, beyond the need for which the information was initially collected.

Privacy risks arise from privacy events—the occurrence or potential occurrence of problematic data actions. The NIST Privacy Framework defines problematic data actions as data actions that may cause an adverse effect for individuals. Problematic data actions might arise by data processing simply for mission or business purposes. Privacy risk is the likelihood that individuals will experience problems resulting from data processing, and the impact should they occur [16]. As reflected in the overlap of Figure 3-1, analyzing these risks in parallel with cybersecurity risks can help organizations understand the full

consequences of impacts of data confidentiality breaches. Section 5.3 demonstrates scenarios where privacy risks may arise and potential mitigations.

Based on the reference architecture, this build considered the data actions that potentially cause problematic data actions.

3.5   Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments,* states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations* [12]—material that is available to the public. The Risk Management Framework (RMF) [13] guidance proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

3.5.1   Security Risk Assessment

Security risk assessments often discuss the consideration of threats to an information system. NIST SP 800-30 Revision 1 defines a threat as "[a]ny circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service". Threats are actions that may compromise a system's confidentiality, integrity, or availability [11]. Threats evolve, and an organization needs to perform its own analysis when evaluating threats and risks that the organization faces.

The following threats were considered during the development of the data confidentiality solution:

- exfiltration by malicious outsider actor
- exfiltration by malicious internal actor (privilege misuse)
- ransomware with threat to leak data
- non-malicious insider actor (accidental email)
- misplaced hardware

For a threat to be realized, a system, process or person must be vulnerable to a threat action. A vulnerability is a deficiency or weakness that a threat source may exploit, resulting in a threat event. Vulnerabilities may exist in a broader context. That is, they may be found in organizational governance structures, external relationships, and mission/business processes.

Organizations should consider impact if a data confidentiality breach occurs including potential decline in organizational trust and credibility affecting employees, customers, partners, stakeholders as well as financial impacts due to loss of proprietary or other sensitive information.

3.5.2 Privacy Risk Assessment

This build also incorporates privacy as part of the build risk assessment. It is important for organizations to address privacy risk as part of a comprehensive risk management process. The build utilized the NIST Privacy Framework [7] and Privacy Risk Assessment Methodology (PRAM) [14] to identify and address privacy risks.

As part of identifying privacy risks in this build, problematic data actions were correlated to observed privacy risks. In many cases, the security capabilities in this build will help mitigate privacy risks, but organizations should use caution to implement these capabilities in a way that does not introduce new privacy risks.

Section 5.3 discusses problematic data action and privacy considerations for this build.

3.6 Technologies

Table 3-1 Products and Technologies lists the technologies used in this project and provides a mapping among the generic application term, the specific product used, and the security control(s) that the product provides. Refer to Table 6-1 Security Control Map for an explanation of the NIST Cybersecurity Framework Subcategory identifiers. Table 3-1 also provides the Privacy Framework Subcategory identifiers, and these are explained in Appendix E.

Table 3-1 Products and Technologies

Component	Product	Capability	NIST Cybersecurity Framework Subcategories	NIST Privacy Framework Subcategories
Data Management	Avrio SIFT v1.0.5.R5	• Discovers, tags, and protects sensitive files across the network	ID.AM-2, PR.DS-1, PR.DS-3	ID.IM-P1, PR.DS-P1, PR.DS-P3
Data Protection	Qcor Forcefield v1.9h	• Protects data at-rest from unauthorized access and malicious modification	PR.DS-1	PR.DS-P1
	PKWARE PKProtect v16.40.0010	• Provides data encryption at-rest and in-transit	PR.DS-1, PR.DS-2	PR.DS-P1, PR.DS-P2
	StrongKey Tellaro	• Provides a Web API (application programming interface) for encryption and tokenization, key management, and strong authentication	PR.AC-7, PR.DS-2	PR.AC-P6, PR.DS-P2
User Access Controls	Cisco Duo	• Provides multi-factor authentication	PR.AC-1, PR.AC-4, PR.AC-7	PR.AC-P1, PR.AC-P4, PR.AC-P6
Browser Isolation	Symantec Web Isolation	• Provides isolation of web browsers to protect from risky traffic • Protects from malware and phishing threats • Provides a privacy toggle that allows for user browsing data to be anonymized. • Provides a login banner to inform individuals of data collection practices with web browsing	PR.AC-5, PR.DS-2	PR.AC-P5, PR.DS-P2, CT.DP-P2, CM.AW-P3
Policy Enforcement	Cisco Duo	• Provides policy control on a global or per-application basis	PR.IP-5	PR.PO-P4

Component	Product	Capability	NIST Cybersecurity Framework Subcategories	NIST Privacy Framework Subcategories
Logging	FireEye Helix	• Provides a baseline for normal enterprise operations • Provides logs and enables incident response	ID.RA-1, ID.RA-2, ID.RA-3, PR.PT-1	CT.DM-P8
Network Protection	Dispel	• Provides remote access to network	PR.AC-3, PR.AC-5	PR.AC-P3, PR.AC-P5

4 Architecture

This section presents the high-level architecture and a set of capabilities used in our data confidentiality reference design that identifies and protects assets from unauthorized access and disclosure.

Figure 4-1 High Level Architecture
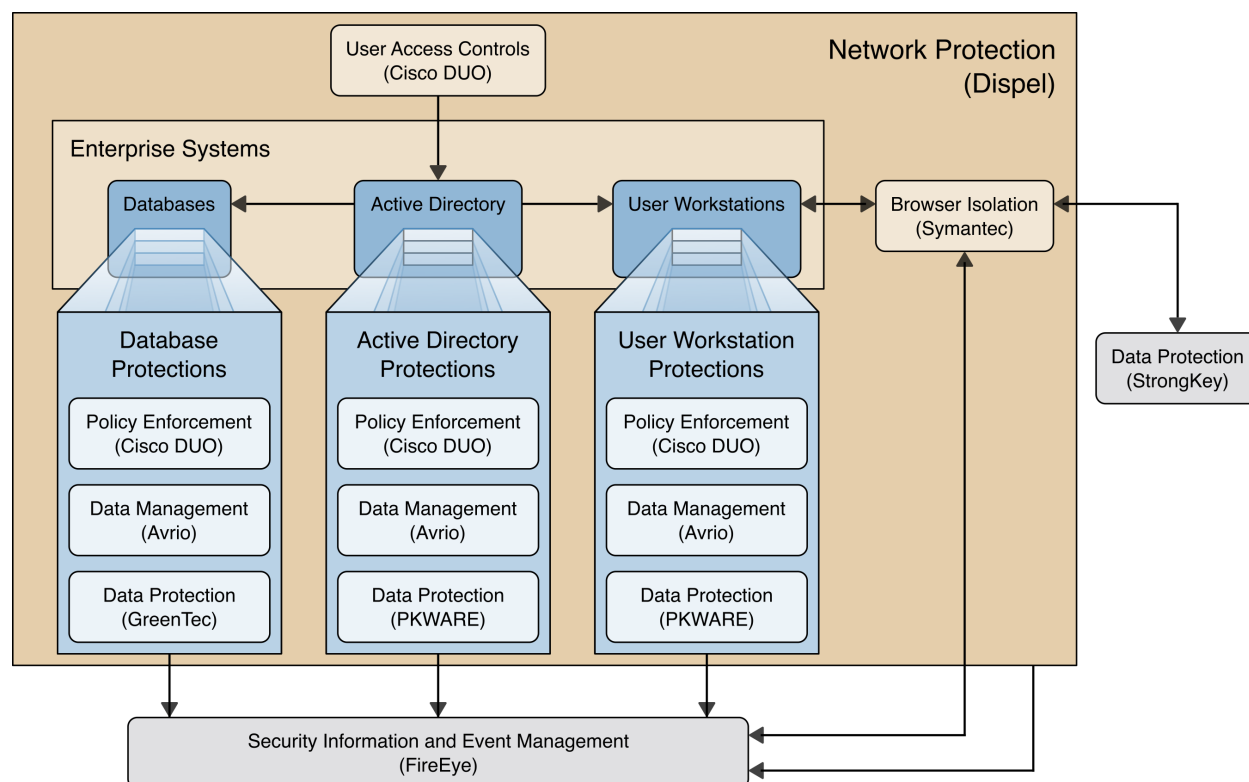
Each of the capabilities implemented plays a role in mitigating data confidentiality attacks:

- **Data Management** allows discovery and tracking of files throughout the enterprise.
- **Data Protection** involves encryption and protection against disclosure of sensitive files.
- **Access Controls** allows organizations to enforce access control policies, ensuring that only authorized users have access to sensitive files.
- **Browser Isolation** protects endpoints in the organization from malicious web-based malware by sandboxing and containing executables downloaded from the internet.
- **Policy Enforcement** ensures that endpoints in the organization conform to specified security policies, which can include certificate verification, installed programs, and machine posture.
- **Logging** creates a baseline of a normal enterprise activity for comparison in the event of a data confidentiality event.
- **Network Protection** ensures that hosts on the network only communicate in allowed ways, preventing side-channel attacks and attacks that rely on direct communication between hosts. Furthermore, it protects against potentially malicious hosts joining or observing traffic (encrypted or decrypted) traversing the network.

These capabilities work together to provide the functions Identify and Protect for the reference architecture. The data management capability provides data inventory and asset management for files in the enterprise; helps identify potentially sensitive files; and works with the data protection capability to ensure potentially sensitive files are properly protected in the event of a breach. Because organizations can be large and new sensitive files may be created daily, it is important to have the capability to automate identification and protection of files at least partially. The data protection capability and access controls prevent data from being read by unauthorized parties. By ensuring that only the correct users and systems have access to data, and that data is protected in-use and at-rest, it becomes more difficult for adversaries to steal and disclose sensitive data.

The policy enforcement, network protection, and browser isolation capabilities work together to protect endpoints such as laptops and desktops against common attack vectors. Malicious websites distributing malware first pass through the browser isolation capability, which sandboxes webpages to ensure that malware downloaded via malicious webpage cannot spread to the user or enterprise's system. Network segmentation uses network layer policies to group endpoints into segments based on business needs. If an endpoint is infected, network segmentation can limit impact by preventing malware from spreading between segments. Policy enforcement ensures that systems remain up to date with organizationally defined security policies. All of these functions feed into logging capabilities and provide organizations with an understanding of their baseline of normal activity. These logs inform the organization of its security posture before an event, so that the organization can adjust its policies as new information about threats becomes available and take appropriate action.

5 Security & Privacy Characteristic Analysis

The following section is intended to help organizations understand the extent to which the project meets its objective of demonstrating technologies and capabilities to help organizations mitigate data confidentiality risk. To support this, we developed several scenarios which organizations may consider when conducting their security and privacy risk analysis. For each scenario we discuss how our architecture might help mitigate or limit security and privacy risks.

5.1 Assumptions and Limitations

The following analysis has the following limitations:

- It is neither a comprehensive test of all security and privacy components, nor a red-team exercise.

- It cannot identify all weaknesses or risks.

- It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture.

5.2 Security Scenarios

Our security evaluation involved assessing how well the reference design addresses the security characteristics that it was intended to support. Each scenario lays out a potential cybersecurity event and discusses the responsibilities of an organization with respect to each event, and how the security

capabilities of our architecture would help an organization address the Cybersecurity Framework Functions of **Identify** and **Protect** for that event.

Below is a list of the scenarios created to test the security capabilities of this architecture.

NOTE: The below scenarios map to the DRAFT NIST CSF 2.0. For a mapping to the NIST CSF 1.1 please see Security Control Map in Appendix D.

5.2.1 Exfiltration of Encrypted Data

Table 5-1 Exfiltration of Encrypted Data Security Scenario

Description	An organization has unknowingly acquired a compromised machine from an outside source and has attached the machine to its trusted network. This machine periodically scans a certain part of the filesystem, which it has deemed to be potentially sensitive, and encrypts and uploads the contents to a malicious web host. Because the machine was assumed to be trusted due to human error, the delivery of this malware into the system is difficult to detect; it must be detected and stopped after it has already started running.
Associated DRAFT CSF 2.0 Subcategories	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-5, ID.RA-5, PR.AA-01, PR.AA-02, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-04
Organizational Response	In this scenario, the organization accepts an infected machine onto its network. As an example, this could be hardware ordered from a third-party vendor, potentially having been refurbished or modified before delivery to the organization. Because the organization connects the machine directly to the network, the acquisition of the malware happens immediately and without warning. It falls to the organization to protect sensitive data from this breach, as well as be able to identify the traffic generated by the malware as anomalous.
Identify	The **Data Management** capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk of targeting and the impact to the enterprise in the event of compromise.
Protect	The **Data Protection** capability provides encryption for sensitive data which has been identified as important, protecting it from unauthorized access in the event of an exfiltration attack.

Another important aspect of the Protect function is the documentation of audit logs, with respect to sensitive data. The **Logging** capability provides a baseline for normal enterprise activity. This baseline can be used as a comparison point in the Detect phase to discover anomalies in network traffic and lead to the discovery of malicious exfiltration. |

5.2.2 Spear Phishing Campaign

Table 5-2 Spear Phishing Campaign Security Scenario

Description	**An unknown user has successfully launched a spear phishing attack, and in the process retrieved an authorized user's login and password. This user has access to several of the organization's databases, allowing them to both view and manipulate the data contained within. This exposes proprietary data to theft and manipulation/deletion.**
Associated DRAFT CSF 2.0 Subcategories	PR.AA-01, PR.AA-02, PR.AA-03, PR.DS-01, PR.DS-02, PR.PS-01, PR.PS-04, DE.CM-09
Organizational Response	In this scenario, someone at the organization with privileged credentials has had their credentials compromised through a spear phishing email. The user may report this themselves if they retroactively realize it was a phishing attack, or they may not. The organization will need to deal with a privileged user account with access to the database being used by a malicious actor and is responsible for protecting assets from the compromised account.
Identify	Though identifying assets is an important function, in this scenario we are specifically focusing on the ability of a compromised user to access an in-use database, and do not have a specific need to identify the database as part of the scenario's resolution, since the target is known.
Protect	The **Data Protection** capability provides write-protection against alteration or deletion of saved data, as well as protection against reading the data through encryption of data-in-use. Another important aspect of the Protect function is the management of access permissions. The **User Access Controls** capability allows the database to be protected by a second layer of authentication separate from the user's username and password. In the event of compromised credentials, the database is less likely to be impacted if two factors of authentication are required. Furthermore, acquisition of user credentials does not necessarily imply that a user's physical system has been stolen. **Policy Enforcement** can take advantage of this by authenticating the hardware, software and/or firmware that is being used by the account at time of access. This is typically done by digital certificates, hash values, or other forms of attestation that are stored in hardware-backed security mechanisms. This serves to ensure that a stolen username and password is not enough to compromise critical resources.

5.2.3 Ransomware

Table 5-3 Ransomware Security Scenario

Description	**An employee of the company makes a mistake while entering the URL of their company's email provider. This mistake takes them to an identical login page, but it is hosted by a malicious actor. When they enter their**

	credentials on the login page, the page records their credentials, and forwards them to the actual login page, as if the credentials were mistyped. The malicious actor later uses these credentials to login as the employee. They download and run a malicious ransomware executable as the user. The ransomware executable uploads sensitive files to the malicious host website, which displays a notice that unless a ransom is paid, the sensitive files will remain publicly visible.
Associated DRAFT CSF 2.0 Subcategories	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-5, ID.RA-5, PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, PR.IR-01, PR.PS-01, PR.PS-04
Organizational Response	In this scenario, someone at the organization with privileged credentials has had their credentials compromised through a malicious webpage disguised as the organization's email provider. The user may or may not report the attack, though there may be clues as to its existence - a user with account troubles and traffic going to a domain name very similar to the organization's domain might be enough to send up red flags if noticed. Regardless, the organization will need to deal with a privileged user account being used to download malware and hold the confidentiality of sensitive files ransom.
Identify	The **Data Management** capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk of targeting and the impact to the enterprise in the event of compromise.
Protect	The **Data Protection** capability provides encryption for sensitive data, protecting it from unauthorized access in the event of an exfiltration attack. Even if the data is stolen and released, encryption prevents the data from being used or read.

Another important component of the Protect function is the documentation of audit logs, with respect to sensitive data. The **Logging** capability provides a baseline for normal enterprise activity. This baseline can be used as a comparison point in the Detect phase to discover anomalies in network traffic and user behavior, potentially allowing for the detection of a malicious actor accessing the user's workstation outside of normal hours.

Browser Isolation, in tandem with **Network Protection,** will prevent downloads of malicious files from websites and unknown ports, limiting the attacker's ability to acquire their ransomware program after the system has been compromised. While the ability to download malicious programs onto the workstation may not completely stop determined attackers, it increases the difficulty and time required for the attack, allowing more time for Detection and Respond activities by the defending organization. |

5.2.4 Accidental Email

Table 5-4 Accidental Email Security Scenario

Description	**A user of the organization accidentally cc's an individual on an email. This email has an attachment containing proprietary information which the cc'd individual is not cleared for. The individual copied on the email is considered a disgruntled employee, and when he sees this email, immediately downloads and saves these files.**
Associated DRAFT CSF 2.0 Subcategories	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-5, ID.RA-5, PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, PR.IR-01, PR.PS-04
Organizational Response	In the event of an accidental information leak via email, it is not unlikely that the event will be reported. Since there are multiple parties involved who are not malicious, it is possible that one of them will report the incident. Regardless of whether it is reported, however, the organization should be able to track the transfer of sensitive data to the unauthorized employee's system, and also prevent that employee from reading it.
Identify	The **Data Management** capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk and the impact to the enterprise in the event of an information leak.
Protect	The **Data Protection** capability provides encryption for sensitive information, protecting it from unauthorized access even if it is accidentally sent to unauthorized users. Another important component of the Protect function is documentation of audit logs, with respect to sensitive data. The **Logging** capability provides a baseline for normal enterprise activity. This baseline can be used as a comparison point in the Detect phase for reporting on data which has been transferred onto the systems of unauthorized users.

5.2.5 Lost Laptop

Table 5-5 Lost Laptop Security Scenario

Description	**A user has lost their work laptop, which contains proprietary information. It is unknown if the laptop was targeted for its data and access credentials by a malicious actor, or if the incident was an unfortunate accident. For the purposes of this scenario, we assume the user of the laptop has reported the missing system on their own.**
Associated DRAFT CSF 2.0 Subcategories	ID.AM-01, ID.AM-02, ID.AM-05, ID.AM-07, PR.AA-01, PR.AA-03, PR.DS-01, PR.DS-09, PR.PS-03
Organizational Response	In the event of a lost laptop, it is likely that the loss will be reported by the user, as the user will directly lose their ability to work. Although some aspects of this event are easier because of the user's knowledge of the system, it is important for the organization to determine the data that was on the laptop, the security posture of the laptop, and the access the laptop

	provided to the organization's network, so that the loss can be accurately assessed, and further data loss can be prevented.
Identify	The Data Management capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk and the impact to the enterprise in the event of a compromise.

The Policy Enforcement capability can be used to force computers connecting to organizational resources to meet requirements regarding which programs are installed. While this capability typically falls under the Protect function, knowing the security posture of assets in the enterprise is an important Identify function. When policy enforcement is used to ensure the presence of encryption capabilities, for example, the enterprise has some assurance that data on the workstation has not been compromised. |
| **Protect** | The Data Protection capability provides encryption for the laptop and prevents sensitive data from being read.

Another important aspect of the Protect function is the management of access permissions. The User Access Controls capability allows the network to be protected by two layers of authentication. Although the laptop may be compromised, requiring user account credentials as well as a second factor of authentication protects the network from further compromise.

Policy Enforcement can be used to force computers connecting to organizational resources to meet requirements regarding which programs are installed, which helps to ensure that lost or stolen machines will have adequate data protection and user access control in place to prevent the loss of data in the event of a lost or stolen laptop. |

5.2.6 Privilege Misuse

Table 5-6 Privilege Misuse Security Scenario

Description	**A malicious insider navigates to one of the organization's shared drives, and finds sensitive information stored there. Looking to sell this information to competitors, the insider copies the information to his personal USB (universal series bus) drive. The insider also prints these files.**
Associated DRAFT CSF 2.0 Subcategories	ID.AM-01, ID.AM-02, ID.AM-05, ID.AM-07, ID.RA-03, PR.AA-03, PR.AA-05, PR.AA-06, PR.DS-01, PR.DS-02, PR.DS-09, PR.PS-04, PR.IR-01
Organizational Response	It is unlikely that a malicious insider will advertise their misdoings; it falls to the organization to discover the insider behavior and protect assets from them. Through proper access control and encryption of sensitive files, organizations can hinder the insider's attempt to exfiltrate useful data. It is unlikely that an organization will be able to completely stop a determined insider through technical means; however, organizations should use the technical capabilities they have to limit the exfiltration, while also gathering

	information about the extent of the loss to aid in the pursuit of legal resolutions to the incident.
Identify	The **Data Management** capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk and the impact to the enterprise in the event of a compromise. In the event of a malicious insider attempting to exfiltrate data, it is important to know which data was accessible on the machines accessed by the insider, as well as the sensitivity levels of the affected data.
Protect	The **Data Protection** capability provides encryption for sensitive data, protecting it from unauthorized access. While a malicious insider may be able to decrypt data relevant to their work role, irrelevant data which is encrypted and managed properly will be significantly less useful to the insider. Another important capability within the Protect Function is the management of access permissions. The **User Access Controls** can prevent unauthorized users from accessing sensitive files in the first place, preventing copying and printing functionality. While user access controls and data protection ensure that the user only has access to some data, ultimately, malicious insiders tend to have some level of access to data due to their role in the organization. **Logging** provides a baseline for normal enterprise activity. This baseline can be used as a comparison point in the Detect phase for reporting on data which has been exfiltrated from the organization. In the event of exfiltration by a malicious insider, logs can help determine what data was accessed and printed and can aid the organization in recovering from the exfiltration, potentially in non-technical ways, such as through the legal system or law enforcement.

5.2.7 Eavesdropping

Table 5-7 Eavesdropping Security Scenario

Description	A malicious outsider has gained access to the network traffic of the organization. They possess the capability to intercept and hijack internal communications via man-in-the-middle attack. A user begins uploading a sensitive proposal for a new project. The malicious outsider is able to intercept and view these files.
Associated DRAFT CSF 2.0 Subcategories	ID.AM-01, ID.AM-03, ID.AM-07, PR.AA-05, PR.AA-06, PR.DS-01, PR.DS-02, PR.PS-04, PR.IR-01
Organizational Response	In this scenario, an organization will likely be able to see the introduction of a new device on the network. In this example, a user's sensitive upload is stolen while it is in transit. The user may see warnings about HTTPS or invalid certificates due to the nature of the attack, and the organization may notice anomalous traffic going through the new device on the network. The organization is responsible for identifying the new device as

	malicious, protecting data intercepted by it through encryption, and mitigating its ability to communicate with trusted enterprise machines.
Identify	The Data Management capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk and the impact to the enterprise. In this scenario, a new project proposal is created - the data management capability is used to identify the creation of new sensitive data and track it throughout the enterprise.
Protect	The Data Protection capability provides encryption for sensitive data, protecting it from unauthorized access. While a malicious third party on the network may be able to intercept the data in transit, encryption prevents the third party from being able to read the intercepted data.
	Another important component of the Protect Function is the documentation of audit logs, with respect to sensitive data. The Logging capability provides a baseline for normal enterprise activity. This baseline can be used as a comparison point in the Detect phase for noticing anomalous network activity, such as a malicious host on the network acting as a proxy between two systems.
	Network Protection is also an important capability for protecting network traffic from malicious adversaries. Using network segmentation, zero trust, and moving target defense capabilities, unrecognized devices can be prevented from identifying, reconnoitering, and accessing the network or communicating with trusted hosts.

5.3 Privacy Scenarios

The following section describes scenarios an organization may consider when conducting their privacy risk assessment. Based on the reference architecture used in this project each scenario is examined for data actions that give rise to potential privacy problems for individuals. Each table documents problematic data actions taken from the NIST Catalogue of Problematic Data Actions and Problems [16], and lists privacy mitigations mapped to the NIST Privacy Framework [7]. For the privacy risks analyzed, consideration was given to how the data is processed. The specific privacy risks found within the scenarios are derived from the architecture components and the data flows used in this build, but to the extent possible, generalized for organizations using similar components and capabilities.

Organizations may collect information affecting privacy when implementing cybersecurity or privacy-based controls. For example, an organization might implement multi-factor authentication (MFA) using information such as mobile phone number. Even though collecting this information helps to protect systems and data by supporting capabilities like non-repudiation and system auditing, it may also generate privacy risks.

When implementing cybersecurity or privacy-based controls, organizations should consider the benefit a user realizes, both from use of a service and securing that service before processing information

affecting privacy. This benefit can be weighed against the risk posed to both individuals and the organization should a privacy event occur.

For example, using MFA mentioned above, users may feel compelled to provide information affecting privacy, such as their personal phone number for SMS (short messaging service) authentication, to gain access to systems or services. However, if the user is accessing publicly available information, the risk of the misuse of information from collecting personal phone numbers may be greater than the security benefit for protecting the low-sensitivity information. Additionally, if given the option, users may elect to use alternative authentication methods that are less privacy-invasive, such as using a work phone number over a personal number or a hardware MFA authenticator over SMS authentication. The NIST Privacy Risk Assessment Methodology (PRAM) refers to this problematic data action, where the user is compelled to provide information disproportionate to the purpose or outcome of the transaction, as induced disclosure.

Organizations should consider these types of risks as they design and implement systems. As demonstrated in the scenarios below, risk mitigations should be implemented within the design to limit privacy risks. These privacy risk mitigations might include the following, among others:

- Understand where and how information is processed, including collection practices and system components that store and transmit this information (data flows and mapping)
- Understand the risks and benefits of collecting different data elements to determine if it should not be collected
- Keep data only as long as needed for its function and destroy or de-identify it otherwise using proper data lifecycle management practices and in accordance with applicable laws and policies
- Keep personal data segregated in a different repository, when practicable
- Encrypt data at rest, in transit, and in use
- Use role-based access controls
- Consider what measures should be taken to address predictability and manageability before deciding whether data can be used beyond its initial expected and agreed upon use
- Implement privacy-enhancing technologies to increase disassociability while retaining confidentiality and the capability to process data for mission or business purposes

5.3.1 User Login with Multifactor Authentication

Phishing-resistant multifactor authentication is a security best practice. The architecture recommends the use of a password, pin (personal identification number) or biometric with an asymmetric cryptographic key for authentication. However, it is common practice for organizations to offer a variety of MFA solutions. This can include user-owned mobile devices, which may impact privacy risk [17].

Figure 5-1 Multifactor Authentication Data Flow Diagram
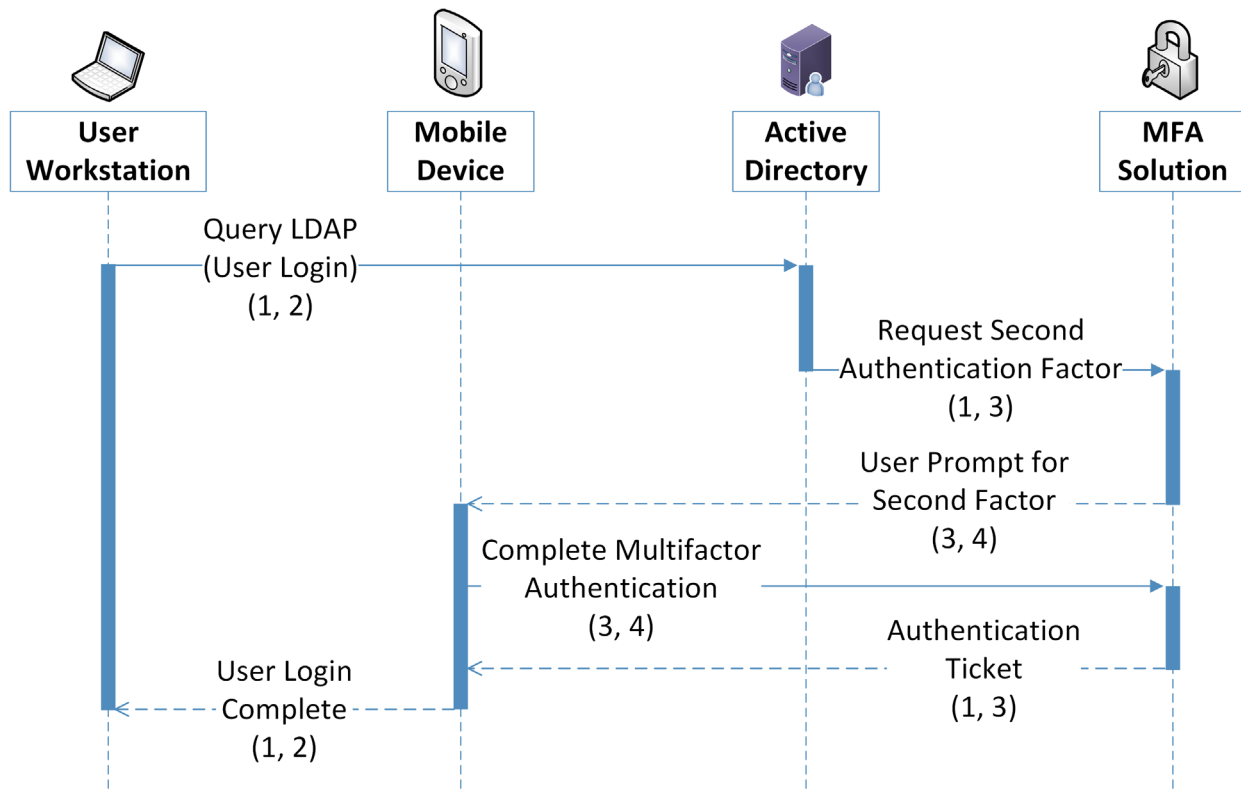
Data Key
1. Username
2. Client IP Address
3. Transaction Identifier
4. Mobile device information (Cellular number)

Table 5-8 User Login with Multifactor Authentication Data Actions

Data Type	Data Action	Privacy Impact
Username	Username is stored by the user workstation and transferred across the authentication process to help identify the transaction.	Usernames potentially contain inferable PII such as user's first and last names.
Client IP Address	The client IP (Internet Protocol) address is stored by the user workstation, and transferred as part of communications where it is an endpoint.	IP addresses can be used to derive PII such as user's general location.
Transaction Identifier	The transaction identifier is generated by active directory and transferred to the MFA solution and the mobile device.	Cross-component identifiers for a transaction can be used to re-identify information that was otherwise anonymized, such as connections between a user's name and their cell phone number.
Mobile device information	The mobile device information is stored by the MFA solution and the mobile device and transferred as a part of the communication between the mobile device and MFA solution.	Information about a user's mobile device, such as device type and version, can be used to infer privacy-impacting information such as the cost of their personal devices. Furthermore, user cell-phone numbers used in certain MFA transactions are PII.

Table 5-9 User Login with Multifactor Authentication Problematic Data Action

Scenarios	Privacy Risk	Problematic Data Actions	Privacy Mitigations
User authentication may use a mobile device as an authenticator, which can be personally or organizationally owned.	Mobile devices are a popular option for authentication processes. Personal information can be transferred in the process of authenticating. This can include phone number and location information. Users' non-work activity may be tracked by an organization.	**Context:** Authentication processes that utilize personally owned mobile devices can require the use of information that is personal to the user, such as phone numbers and other metadata. The tracking could extend beyond the work environment or even within the work environment be disproportionate to the security needs leading to unanticipated revelations about user activities or degradation of the dignity or autonomy of users. **Problematic Data Action:** Unanticipated Revelation, Induced Disclosure **Problem:** Loss of Autonomy: Users have no control over what information is shared in this scheme. Users may not feel comfortable using their own personal information as a security feature for an organizational service. Loss of Trust: Users may not feel comfortable with their personal phone numbers and device information being shared with third-party applications and Software as a Service providers.	**Predictability:** Organizations should inform users of information that is viewed and collected by login tools, such as through privacy notices when devices are enrolled. System administrators should have limited access to user authentication information. **Manageability**: Organizations that leverage user's personal devices for user login processes should consider tools that give the users optionality for registering different types of authenticators, including those that do not use personal devices and information. In this build, Duo offers a variety of authentication options, such as a hardware-based authenticator. Organizations should audit tools to determine what information they are using and collecting. **Disassociability:** Organizations should explore capabilities and configurations that allow for the de-identification of phone numbers and other personal information, such as the capability to replace a phone-number with placeholder text or privacy-enhancing cryptographic techniques to limit the tracking of users.

5.3.2 Authentication to Virtual Desktop Interface Solution

The reference architecture in this document demonstrates a Virtual Desktop Interface (VDI) solution to facilitate secure access to organizational resources and data. Organizations may allow users' personal devices to access corporate resources using the VDI solution. Organizations should consider the privacy risk of installing VDI software on personally owned devices, information revealed by the VDI protocol, and monitoring of user activity while in the virtual environment.

Figure 5-2 Virtual Desktop Interface Data Flow Diagram

Data Key
1. Username
2. Client IP address
3. Token identifier
4. One-time password
5. Client time zone, computer name
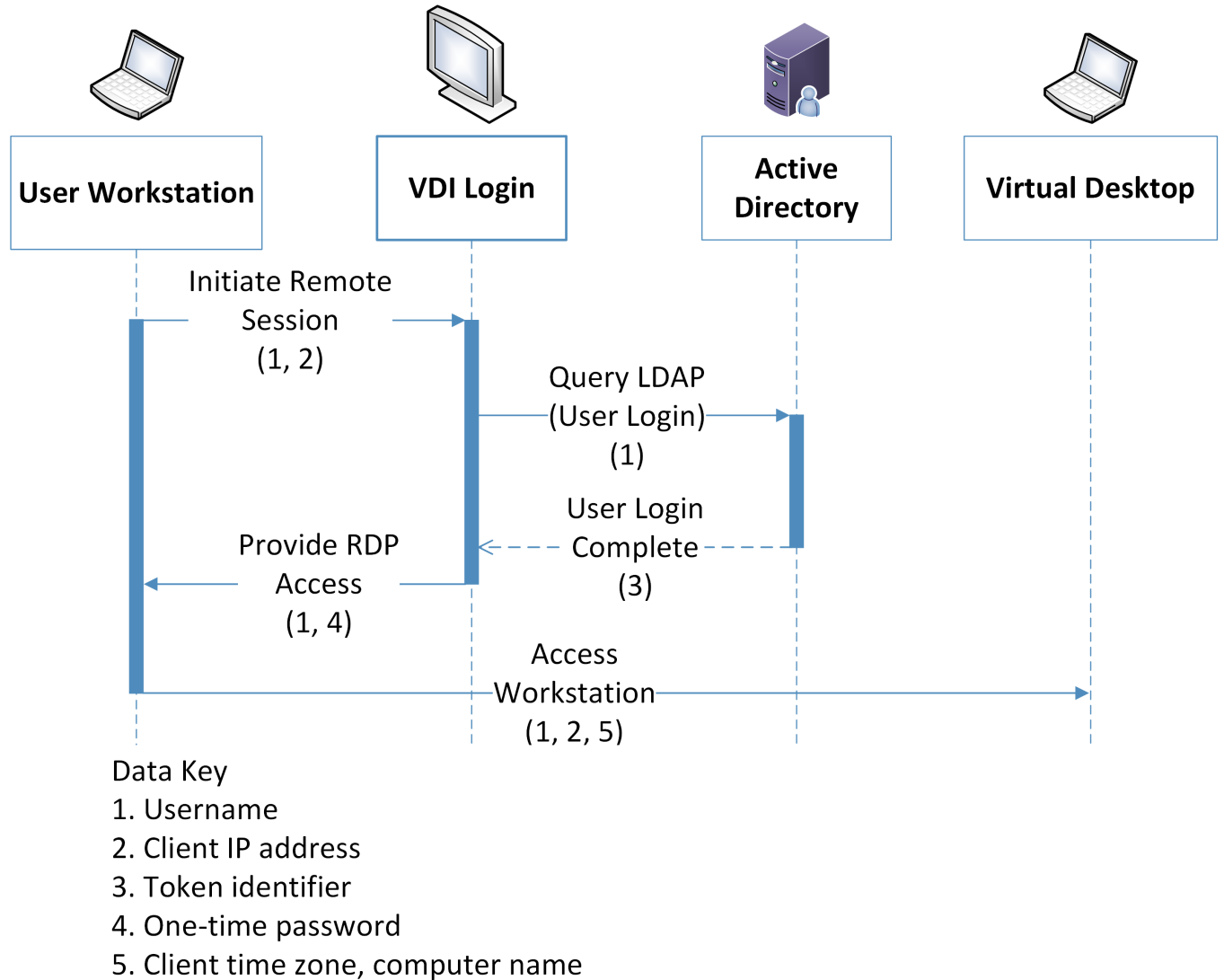
Table 5-10 Virtual Desktop Interface Data Actions

Data Type	Data Action	Privacy Impact
Username	The username is stored by the user workstation and active directory. It is transferred as part of the authentication process.	Usernames potentially contain inferable PII such as user's first and last names
Client IP Address	The Client IP Address is stored on the user workstation, and transferred as part of transactions and connections it generates.	IP addresses can be used to derive PII such as user's general location
Token Identifier	A Token Identifier is generated by Active Directory in support of the authentication process and transferred to the VDI.	Token identifiers can be used to re-identify other information affecting privacy that occur as part of transactions.
One-time password	A One-time Password is generated by the VDI to authenticate the RDP (remote desktop protocol) connection and is transferred to and stored on the user workstation.	
Client Time Zone	The Client Time Zone is stored by the user workstation and transferred as part of an RDP connection to the virtual desktop.	Along with IP addresses, time zones specifically provide information about a user's location
Client Computer Name	The Client Computer Name is stored by the user workstation and transferred as part of an RDP connection to the virtual desktop.	User's personal device names can include inferable PII, such as personal names and device locations.

Table 5-11 Virtual Desktop Interface Problematic Data Actions

| Scenarios	Privacy Risk	Problematic Data Actions	Privacy Mitigations
User logs into a Virtual Desktop Interface solution from a personally or organizationally owned device.	Central login platforms can be connected to by a variety of devices, which may be personally owned by the user. Information that can be associated with the user, such as their device information or location, may be transmitted to security tools as part of the authentication process.	**Context:** Users operating under a BYOD or remote work scheme may not expect that certain data is under organizational purview. This can include their location, personal device metadata, and operating hours. **Problematic Data Action:** Surveillance, Unanticipated Revelation **Problem:** Loss of Trust. Users may not feel comfortable with this information being shared with third-party applications, or the company in general. Dignity Loss. Users may have information, such as their physical location and work hours, revealed to organizations in an undesired fashion.	**Predictability**: Users should be informed of information that is viewed and collected by login and network access tools such as Dispel, through either a login banner or other alert mechanism. Use privacy enhancing technologies and techniques to de-identify user, user ID and IP address like obfuscation, communication anonymization, data minimization, and pseudonymization, among others. **Manageability:** Organizations that include user's personal devices in day-to-day operation should audit tools to determine what information they are using and collecting and who has access rights **Confidentiality**: Organizations should mandate strict access control for the management and configuration of user login services, such as with MFA. **Availability:** Organizations that utilize central login platforms as their entry should consider the robustness of their platforms and systems. A loss of access to these systems can lead to an inability for users to access their data.

5.3.3 Automated Data Movement with Data Management Solution

The reference architecture uses data management technology that allows for the scanning files for highly sensitive information and establishment of policy that automatically moves sensitive content to secure storage. Files with detected PII or other sensitive information may be moved in ways that are unexpected to the user, potentially creating privacy concerns.

Figure 5-3 Data Management Data Flow Diagram
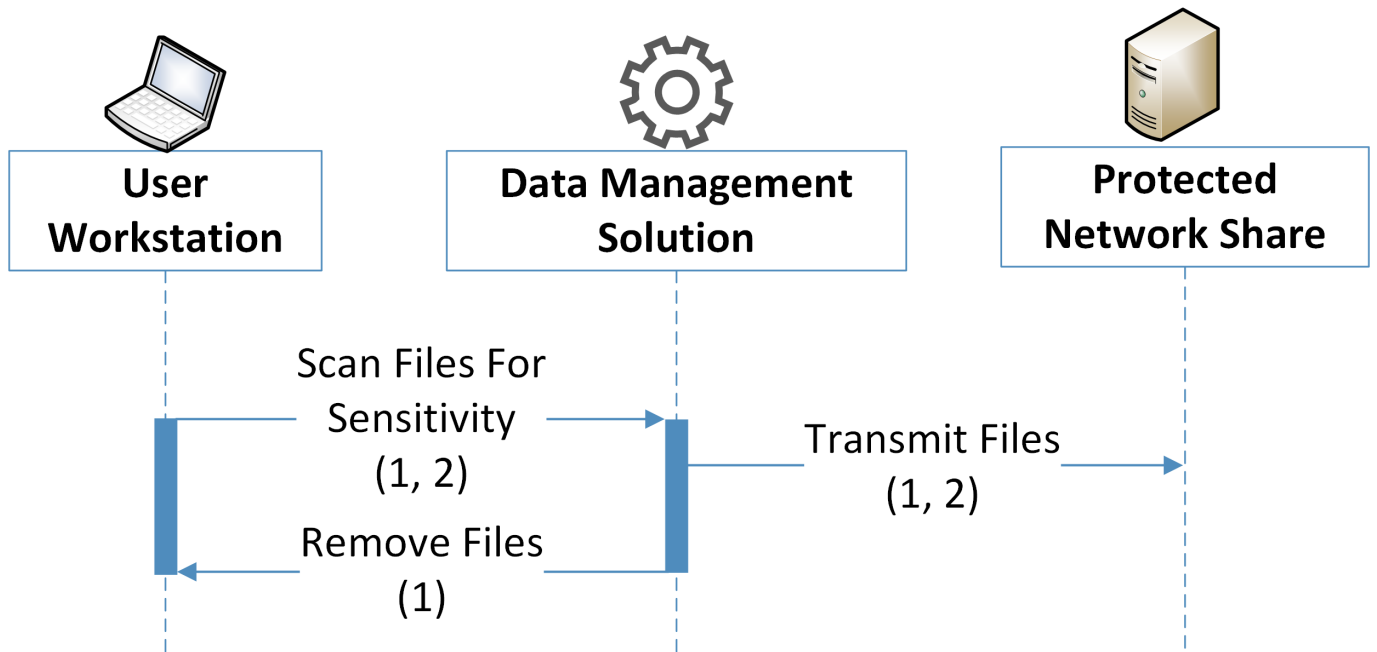
Data Key
1. File metadata (Name, Date of Modification, File Type, Author)
2. File contents

Table 5-12 Data Management Data Action

Data Type	Data Action	Privacy Impact
File metadata	File metadata is stored on the user workstation, along with file contents. It is transferred along with file contents to the Data Management Solution and the Protected Network Share as part of the data movement operation. It is also used to identify data for deletion by the Data Management Solution.	File metadata can include information affecting privacy that is not derivable from file contents, such as the file name, date of modification, and author. This can be used to derive information such as active work hours and can lead to false assumptions about an individual
File contents	File contents are stored on the user workstation and transferred through the Data Management Solution to the Protected Network Share.	The privacy impact of file contents rely heavily on the data being used by an enterprise. This information can include SSNs, credit card information, health data, and other PII. Privacy impact and regulatory burden should be specifically considered and analyzed by organizations implementing these sorts of security solutions.

Table 5-13 Data Management Problematic Data Actions

Scenarios	Privacy Risk	Problematic Data Actions	Privacy Mitigations
Data generated in areas moderated by data management solutions are potentially duplicated, moved, or deleted in compliance with organizational policy.	Movement of data by external tools can lead to information being placed in unexpected or unintended places. This can lead to user confusion and a loss of trust in the organization, as well as data being made vulnerable to discovery and exfiltration	**Context:** Moving data from the place in which it was created or saved can create confusion for users and expose information in ways the user did not intend. **Problematic Data Action:** Appropriation, Unanticipated Revelation **Problem:** Loss of Trust. Users may be uncomfortable working in protected zones if they do not trust that their data will be kept under their control. Loss of Autonomy. Users may see involuntary data movement as a loss of their ability to govern the data they generate.	**Predictability**: Zones under the purview of data management and protection tools should be clearly defined and expressed to the user, such as through clearly understood network share names. Notice should be given to users who are impacted by the data management solution, such as by leaving a stub file at the original location. **Manageability:** Organizations seeking to include these capabilities should make sure they use solutions that can be configured to mitigate their inherent privacy risk. **Confidentiality**: Tools that provide the ability to analyze and move data should only be governed by system administrators. The automatic movement of data should only move data to locations only accessible by the user who created the original data or to folder with equal or more stringent access rights than the originating location. Furthermore, data locations are protected by IDAM (identity and access management controls) controls such as MFA.

5.3.4 Monitoring by Logging Solution

This reference architecture generates logs used to aid in response and recovery activities. These logs are essential for proper data management and incident response. However, organizations should consider the privacy of information collected by logs when they are created, transmitted, and stored.

Figure 5-4 Logging Data Flow Diagram
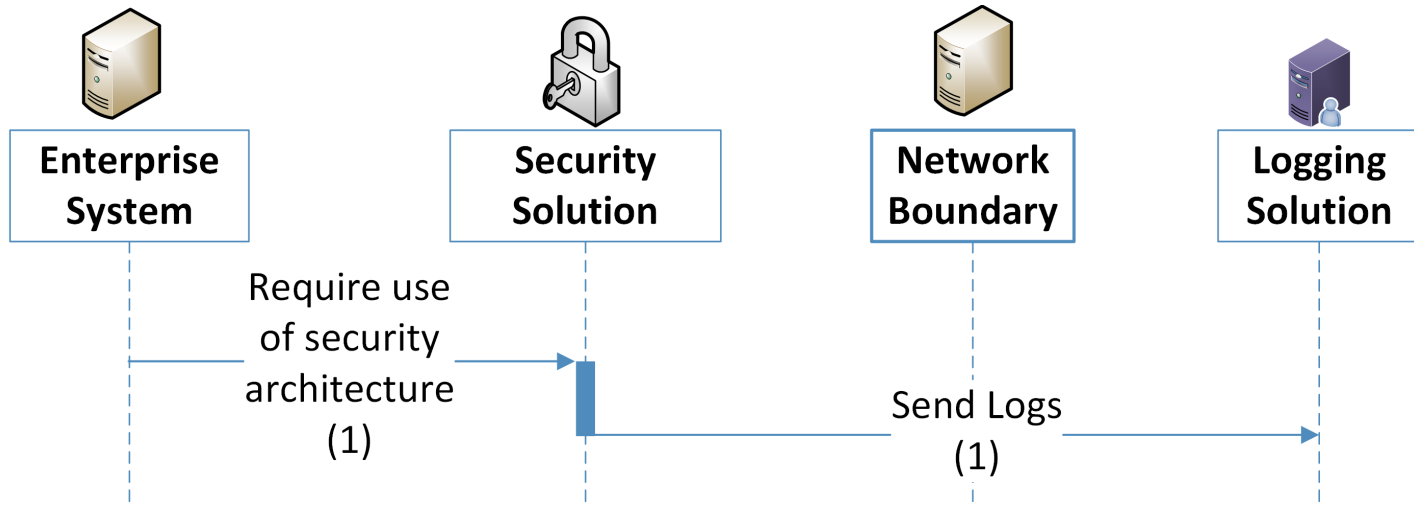
Data Key
1. Usernames, IP addresses, web traffic history

The utilization of the security architecture, and the logs their user generates, can interact with and generate information that affects privacy. The use of a logging solution requires that data and metadata about user's activity be generated and stored in an additional location. Depending on the details and scope of the logging tool, this can extend the effective domain of information that affects privacy used by those tools. Some examples of information affecting privacy utilized in such transactions is given below:

Table 5-14 Logging Data Actions

Data Type	Data Action	Privacy Impact
IP Addresses	IP Addresses are stored and transferred by enterprise systems as well as the logging solution. They are transferred by and through the security solutions.	IP addresses can be used to determine rough locations for user-owned machines. Additionally, IP Addresses can be common across logs from many security tools, allowing for anonymized data to be re-identified.
Device Identifiers	Device Identifiers are stored and transferred by enterprise systems as well as the logging solution. They are transferred by and through the security solutions.	Under certain circumstances, device Identifiers, such as MAC (media access control) addresses, can be used to identify individuals from data that has been de-identified, or allow for privacy-impacting correlations to be made between data logs.

Table 5-15 Logging Problematic Data Actions

Scenarios	Privacy Risk	Problematic Data Actions	Privacy Mitigations
Security tools generate metadata that is transferred to a logging solution, either directly or via an on-site forwarder.	The security system passively creates data about users, their data, and their activities. This information is transmitted across the network and stored remotely.	**Context:** Logging systems can contain private data. These logs are transmitted off the device or system in which they were created to other systems where log information is aggregated. The privacy impact of each log and the aggregation of logs must be considered. Furthermore, this information is exposed to admin user who have access to either the individual or aggregated logs. **Problematic Data Action:** Unanticipated Revelation, Re-identification, Surveillance **Problem:** Loss of trust. Users may not expect the scope of information created and tracked by logs, even if they understand the scope of the security infrastructure. Dignity Loss. Embarrassing or undesired privacy information may be inferred about individuals whose actions generate logging information.	**Predictability:** The existence of monitoring systems should be disclosed to users upon their access to organizational systems, such as through a login banner. Use privacy enhancing technologies and techniques to de-identify user ID and IP address like obfuscation, communication anonymization, data minimization, and pseudonymization, among others. **Manageability:** Organizations should evaluate how logs can be configured to collect the least amount of information necessary in order to meet security needs, especially when security tools are aggregating log information across multiple systems. **Disassociability:** Organizations should consider de-identification functions for log creation, transmission, storage and aggregation. For example, privacy-relevant information such as the user's name can be disassociated from their IP address or device identifier when collecting log information. **Confidentiality:** Tools that generate or store logs should have strict access control applied to them such as MFA.

5.3.5 User Web Browsing with Browser Isolation Solution

Web isolation solutions must have governance over all user web traffic to be effective. This can generate privacy concerns to users by increasing the risk of their browsing data being misused.

Figure 5-5 Browser Isolation Data Flow Diagram

Data Key
1. Client IP Address
2. User browsing metadata (Target IP address, URL, Session information)
3. User browsing contents
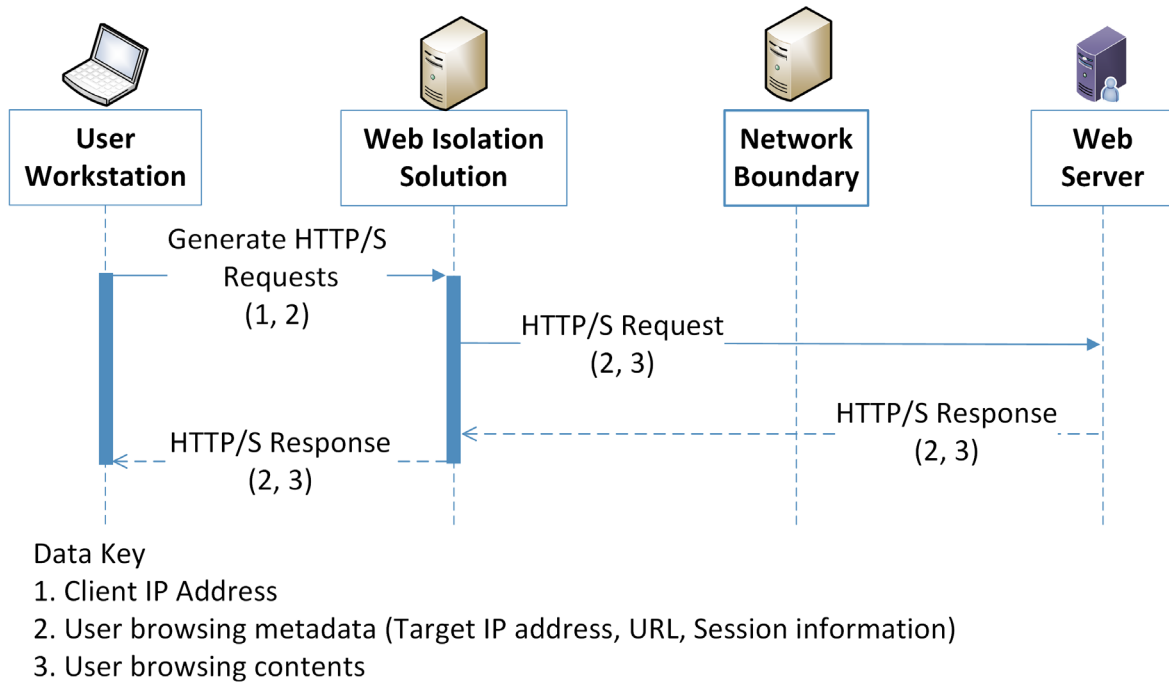
Table 5-16 Browser Isolation Data Actions

Data Type	Data Action	Privacy Impact
Client IP Address	IP Addresses are stored on the User Workstation and sent by network connections to and from it.	IP addresses can be used to derive PII such as a user's general location
User browsing metadata	User browsing metadata is generated on the user workstation and sent to and from the user workstation, as well as to and from the web isolation solution to the web server.	HTTP/S traffic, even when encrypted, relies on unencrypted metadata such as time stamps, source IPs, and destination IPs. These materials can be used to generate information that affects privacy, such as a specific user's browsing habits.
User browsing contents	User browsing contents are generated on the user workstation as well as the web server. They are sent back and forth between the web server and the web isolation solution and delivered back to the user workstation.	Tools that can view and inspect the contents of a user's web browsing session could further impact user privacy. This can include a user accessing their bank and checking balance information, accessing information from their healthcare provider, and so on.

Table 5-17 Browser Isolation Problematic Data Actions

Scenarios	Privacy Risk	Problematic Data Actions	Privacy Mitigations
Data from user web browsing flows through web isolation solutions, centralizing information about employee web browsing.	Web monitoring tools are used to detect malicious web traffic patterns or access requests to unsafe domains but may also collect and transmit information that affects the user's privacy.	**Context:** User browsing data can reveal information affecting privacy, such as personal health or financial information. Administrators can centrally view user browsing metadata at this location. This information may also be forwarded to other third-party tools. **Problematic Data Action:** Surveillance, Unanticipated Revelation **Problem:** Loss of Trust. Users may perceive the monitoring of their web traffic as a form of surveillance which may negatively impact the trust they have in their IT systems and/or organization.	**Predictability**: Users should be informed on the capabilities of web monitoring and related tools, such as through a login banner. Use privacy enhancing technologies and techniques to de-identify user ID and IP address like obfuscation, communication anonymization, data minimization, and pseudonymization, among others. **Manageability:** Organizations seeking to use web monitor tools should assess their privacy preserving capabilities. In this reference architecture Symantec Web Isolation provides a privacy toggle that allows for user browsing data to be anonymized. **Disassociability**: Organizations should employ de-identification options for data when appropriate. In this reference architecture the privacy toggle provided by Symantec Web Isolation was enabled, which anonymized user browsing data. **Confidentiality:** Organizations should mandate strict access controls for security tools that can impact user privacy, including the use of MFA.

6   Future Build Considerations

As shown in [Figure 1-1](#), the NCCoE Data Security work that remains to be addressed within the framework of the CIA triad is Data Availability. The Data Security team plans to evaluate the current landscape of Data Availability challenges that organizations face and determine future relevant projects to address those needs.

Appendix A   List of Acronyms

API	Application Programming Interface
BYOD	Bring Your Own Device
CIA	Confidentiality Integrity Availability
CIS	Center for Internet Security
CNSSI	Committee on National Security Systems Instruction
COBIT	Control Objectives for Information and Related Technologies
CRADA	Cooperative Research And Development Agreement
CSC	Critical Security Controls
CSF	Cybersecurity Framework
FIPS	Federal Information Processing Standard
FIPPS	Fair Information Privacy Principles
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDAM	Identity and Access Management
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
MAC	Media Access Control
MFA	Multi Factor Authentication
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NIST IR	NIST Interagency or Internal Report
PDA	Problematic Data Action
PII	Personally Identifiable Information
PIN	Personal Identification Number
PRAM	Privacy Risk Assessment Methodology
RDP	Remote Desktop Protocol
RMF	Risk Management Framework
SMS	Short Messaging Service
SP	Special Publication
URL	Uniform Resource Locator
USB	Universal Series Bus

VDI   Virtual Desktop Interface

Appendix B   Glossary

Access Control   The process of granting or denying specific requests to 1) obtain and use information and related information processing services and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).

SOURCE: Federal Information Processing Standard (FIPS) 201-3

Adversary   Person, group, organization, or government that conducts or has the intent to conduct detrimental activities.

SOURCE: CNSSI 4009-2015

Asset   A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

SOURCE: Committee on National Security Systems Instruction (CNSSI) 4009-2015

Authentication   Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

SOURCE: FIPS 200

Authorization   Access privileges granted to a user, program, or process or the act of granting those privileges.

SOURCE: CNSSI 4009-2015

Breach   The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose.

SOURCE: NIST SP 800-53 Rev. 5

Control   The means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature.

SOURCE: NIST SP 800-160 Vol. 2 Rev. 1

Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
	SOURCE: FIPS 200
Data	A subset of information in an electronic format that allows it to be retrieved or transmitted.
	SOURCE: CNSSI 4008-2015
Data Action	A system/product/service data life cycle operation, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal.
	SOURCE: NIST Privacy Framework Version 1.0
Disassociability	Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system.
	SOURCE: NISTIR 8062
Encrypt	Cryptographically transform data to produce cipher text.
	SOURCE: CNSSI 4009-2015
Enterprise	An entity of any size, complexity, or positioning within an organizational structure.
	SOURCE: NIST SP 800-72
Event	Any observable occurrence in a network or system.
	SOURCE: CNSSI 4009-2015
Exfiltration	The unauthorized transfer of information from an information system.
	SOURCE: CNSSI 4009-2015
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
	SOURCE: FIPS 200

Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. SOURCE: FIPS 200
Key Management	The activities involving handling of cryptographic keys and other related security parameters (e.g. passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction. SOURCE: CNSSI 4009-2015
Manageability	Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure. SOURCE: NISTIR 8062
Malware	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. SOURCE: CNSSI 4009-2015
Mitigation	A decision, action, or practice intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities. SOURCE: NIST SP 1800-160 Vol. 2 Rev. 1
Multi-Factor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). SOURCE: CNSSI 4009-2015
Phishing	A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. SOURCE: CNSSI 4009-2015
Predictability	Enabling reliable assumptions by individuals, owners, and operators about PII and its processing by a system. SOURCE: NISTIR 8062

Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. SOURCE: FIPS 200
Security Control	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information. SOURCE: NIST SP 800-53
Security Policy	A set of rules that governs all aspects of security-relevant system and system component behavior. SOURCE: NIST SP 800-53 Rev. 5
Spear Phishing	A colloquial term that can be used to describe any highly targeted phishing attack. SOURCE: CNSSI 4009-2015
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. SOURCE: NIST SP 800-53 Rev. 5
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. SOURCE: FIPS 200

Appendix C   References

[1]   W. Barker, *Guideline for Identifying an Information System as a National Security System*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-59, Gaithersburg, Md., Aug. 2003, 17 pp. Available: https://doi.org/10.6028/NIST.SP.800-59.

[2]   T. McBride *et. al*, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-25, Gaithersburg, Md., Dec. 2020, 488 pp. Available: https://doi.org/10.6028/NIST.SP.1800-25.

[3]   T. McBride *et. al*, *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*, National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-26, Gaithersburg, Md., Dec. 2020, 441 pp. Available: https://doi.org/10.6028/NIST.SP.1800-26.

[4]   T. McBride *et. al*, *Data Integrity: Recovering from Ransomware and Other Destructive Events*, National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-11, Gaithersburg, Md., Sep. 2020, 377 pp. Available: https://doi.org/10.6028/NIST.SP.1800-11.

[5]   M. Souppaya and K. Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-83 Revision 1, Gaithersburg, Md., July 2013, 36 pp. Available: https://doi.org/10.6028/NIST.SP.800-83r1.

[6]   M. Souppaya and K. Scarfone, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Devise (BYOD) Security*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46 Revision 2, Gaithersburg, Md., July 2016, 43 pp. Available: https://doi.org/10.6028/NIST.SP.800-46r2.

[7]   NIST. *Privacy Framework*. Available: https://www.nist.gov/privacy-framework.

[8]   NIST. *Cybersecurity Framework*. Available: http://www.nist.gov/cyberframework.

[9]   W. Barker *et. al*, *Ransomware Risk Management: A Cybersecurity Framework Profile*, NIST Interagency Report 8374, Gaithersburg, Md., Feb. 2022, 23 pp. Available: https://doi.org/10.6028/NIST.IR.8374.

[10] R. Ross *et. al*, *Developing Cyber-Resilient Systems: A Systems Security Engineering* Approach, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160 Volume 2 Revision 1, Gaithersburg, Md., Dec. 2021, 309 pp. Available: https://doi.org/10.6028/NIST.SP.800-160v2r1.

[11] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Revision 1, Gaithersburg, Md., Sep. 2012, 83 pp. Available: https://doi.org/10.6028/NIST.SP.800-30r1.

[12] Joint Task Force, *Risk Management Framework for Information Systems and Organizations*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 2, Gaithersburg, Md., Dec. 2018, 164 pp. Available: https://doi.org/10.6028/NIST.SP.800-37r2.

[13] NIST. *Risk Management Framework*. Available: https://csrc.nist.gov/projects/risk-management/about-rmf.

[14] NIST. *Privacy Risk Assessment Methodology*. Available: https://www.nist.gov/privacy-framework/nist-pram.

[15] S. Brooks *et. al*, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, NIST Interagency Report 8062, Gaithersburg, Md., Jan. 2017, 41 pp. Available: https://doi.org/10.6028/NIST.IR.8062.

[16] NIST. *Catalog of Problematic Data Actions and Problems*. Available: https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM/catalog-PDAP.md.

[17] NIST Cybersecurity Center of Excellence, Mobile Device Security, Bring Your Own Device Practice Guide, NIST SP 1800-22, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-22.pdf.

[18] NIST Privacy Framework Repository, https://www.nist.gov/privacy-framework/resource-repository.

Appendix D   Security Control Map

The following table lists the NIST Cybersecurity Framework Functions, Categories, and Subcategories addressed by this project and maps them to relevant NIST standards, industry standards, and controls and best practices.

Table 6-1 Security Control Map

Cybersecurity Framework v1.1			Standards & Best Practices
Function	**Category**	**Subcategory**	**Informative References**
IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-2: Software platforms and applications within the organization are inventoried	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
	Risk Assessment (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	CIS CSC 4 COBIT 5 BAI08.01 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16

Cybersecurity Framework v1.1			Standards & Best Practices
Function	**Category**	**Subcategory**	**Informative References**
		ID.RA-3: Threats, both internal and external, are identified and documented	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM16
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	CIS CSC 1, 5, 15, 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-3: Remote access is managed	CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC5, AC-6, AC-14, AC-16, AC-24

Cybersecurity Framework v1.1			Standards & Best Practices
Function	**Category**	**Subcategory**	**Informative References**
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	CIS CSC 1, 12, 15, 16 COBIT 5 DSS05.04, DSS05.10, DSS06.10 ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9
	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected	CIS CSC 13, 14 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 ISA 62443-3-3:2013 SR 3.4, SR 4.1 ISO/IEC 27001:2013 A.8.2.3 NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28
		PR.DS-2: Data-in-transit is protected	CIS CSC 13, 14 COBIT 5 APO01.06, DSS05.02, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12

Cybersecurity Framework v1.1			Standards & Best Practices
Function	Category	Subcategory	Informative References
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	CIS CSC 1 COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
	Information Protection Processes and Procedures (PR.IP)	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	CIS CSC 10 COBIT 5 APO13.01, DSS01.01, DSS04.07 ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
	Protective Technology (PR.PT)	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	CIS CSC 1, 3, 5, 6, 14, 15, 16 COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 AU Family

Appendix E   Privacy Control Map

The following table lists the NIST Privacy Framework Functions, Categories, and Subcategories addressed by this project and maps them to relevant NIST standards, industry standards, and controls and best practices.

NOTE: The International Organization for Standardization (IS0) standard 27701 references were not mapped by NIST, but by an external organization. They are available at the NIST Privacy Framework Repository [18] and provided here for convenience. The Fair Information Privacy Principles (FIPPS) references are provided to aid understanding of the Privacy Control Map.

Table 6-2 Privacy Control Map

Privacy Framework 1.0			Standards and Best Practices
Function	**Category**	**Subcategory**	**Informative Refences**
IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.	**ID.IM-P1:** Systems/products/services that process data are inventoried.	**FIPPS 7:** Purpose Specification/Use Limitation **NIST SP 800-37 Rev. 2:** Task P-10 **NIST SP 800-53 Rev. 5:** CM-8 (10), CM-12, CM-13, PM-5 **NIST IR 8062** **NIST PRAM:** Worksheet 2 **ISO/IEC 27701:2019** 7.2.8, 8.2.6
CONTROL-P (CT-P): Develop and Optional (Risk Based) appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.	**Data Processing Management (CT.DM-P):** Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).	**CT.DM-P8:** Audit/log records are determined, documented, and reviewed in accordance with policy and incorporating the principle of data minimization.	**FIPPS 4**: Minimization **NIST SP 800-53 Rev. 5:** AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16 **NIST IR 8062** **ISO/IEC 27701:2019** 6.9.4.1, 6.9.4.2, 6.15.1.3

Privacy Framework 1.0				Standards and Best Practices
	Function	**Category**	**Subcategory**	**Informative Refences**
		Disassociated Processing (CT.DP-P): Data processing solutions increase disasso-ciability consistent with the organization's risk strategy to protect individ-uals' privacy and enable implementation of privacy principles (e.g., data mini-mization).	**CT.DP-P2:** Data are processed to limit the identification of in-dividuals (e.g., de-identification privacy techniques, tokeniza-tion).	**FIPPS 7:** Purpose Specification/Use Limitation **NIST SP 800-53 Rev. 5:** AC-23, AU-3(3), IA-4(8), PE-8(3), SA-8(33), SI-12(1), SI-12(2), SI-19 **NIST SP 800-63-3** **NIST SP 800-188 (draft)** **NIST IR 8053** **NIST IR 8062** **ISO/IEC 27701:2019** 7.4.2, 7.4.4
		Data Processing Aware-ness (CM.AW-P): Individu-als and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mecha-nisms are used and main-tained to increase predict-ability consistent with the organization's risk strategy to protect individuals' pri-vacy.	**CM.AW-P3:** System/prod-uct/service design enables data processing visibility.	**FIPPS 7:** Purpose Specification/Use Limitation **NIST SP 800-53 Rev. 5:** PL-8, PT-5(1), SA-17, SC-42(4) **NIST IR 8062** **ISO/IEC 27701:2019** 7.3.2, 7.3.3, 8.3.1
	PROTECT-P (PR-P): Develop and Implement appropriate data processing safeguards.	**Data Protection Policies, Processes, and Procedures (PR.PO-P):** Security and privacy policies (e.g., pur-pose, scope, roles and re-sponsibilities in the data processing ecosystem, and	**PR.PO-P4:** Policy and regula-tions regarding the physical op-erating environment for organi-zational assets are met.	**FIPPS 5:** Quality and Integrity **FIPPS 7:** Purpose Specification/Use Limitation **NIST SP 800-53 Rev. 5:** PE-1 **ISO/IEC 27701:2019** All of 6.8

Privacy Framework 1.0			Standards and Best Practices
Function	Category	Subcategory	Informative Refences
	management commit-ment), processes, and pro-cedures are maintained and used to manage the protection of data.		
	Identity Management, Au-thentication, and Access Control (PR.AC-P): Access to data and devices is lim-ited to authorized individu-als, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.	**PR.AC-P1:** Identities and cre-dentials are issued, managed, verified, revoked, and audited for authorized individuals, pro-cesses, and devices.	**FIPPS 8: Security** **NIST SP 800-53 Rev. 5:** IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12 **NIST SP 800-63-3** **ISO/IEC 27701:2019** 6.6.2.1, 6.6.2.2, 6.6.4.2
		PR.AC-P3: Remote access is managed.	**FIPPS 8: Security** **FIPS Publication 199** **NIST SP 800-46 Rev. 2** **NIST SP 800-53 Rev. 5:** AC-1, AC-17, AC-19, AC-20, SC-15 **NIST SP 800-77** **NIST SP 800-113** **NIST SP 800-114 Rev. 1** **NIST SP 800-121 Rev. 2** **ISO/IEC 27701:2019** 6.6.2.1, 6.6.2.2
		PR.AC-P4: Access permissions and authorizations are man-aged, incorporating the princi-ples of least privilege and sepa-ration of duties.	**FIPPS 8: Security** **NIST SP 800-53 Rev. 5:** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 **NIST SP 800-162**

Privacy Framework 1.0			Standards and Best Practices
Function	**Category**	**Subcategory**	**Informative Refences**
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	**FIPPS 8: Security** **NIST SP 800-53 Rev. 5:** AC-4, AC-10, SC-7, SC-10, SC-20
		PR.AC-P6: Individuals and devices are proofed and bound to credentials and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	**FIPPS 8: Security** **NIST SP 800-53 Rev. 5:** AC-14, AC-16, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11, IA-12, PE-2, PS-3 **NIST SP 800-63-3**
	Data Security (PR.DS-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.	**PR.DS-P1:** Data-at-rest are protected.	**FIPPS 8: Security** **NIST SP 800-53 Rev. 5:** MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28 **NIST SP 800-175B**
		PR.DS-P2: Data-in-transit are protected.	**FIPPS 8: Security** **NIST SP 800-53 Rev. 5:** SC-8, SC-11 **NIST SP 800-175B**
		PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.	**FIPPS 8: Security** **NIST SP 800-53 Rev. 5:** CM-8, MP-6, PE-16, PE-20