REIMAGINING OCA'S DIVISION OF TECHNOLOGY

A STRATEGIC REORGANIZATION

TABLE OF CONTENTS

LIST OF EXHIBITS

INTRODUCTION

New York Courts, indeed, all modern organizations, operate in two distinct parallel environments—the physical and the digital. Over the past two decades, the digital environment has expanded from a subset of our physical world to occupy an entirely new plane of virtual existence, with its unique structure, rules and operational hurdles governing operations not only within our court system but expanding into the general public.

To date, New York Courts ("the courts") have sought to meet the challenges of digital operations by growing organically as technologies and needs arose. The Office of Court Administration ("OCA") boasts a team of capable professionals with many of the skills necessary to meet the growing challenges of digital life. Recent events have made clear, however, that the exigencies of digital operations require greater agility and strategic planning than previously understood. New York Courts, therefore, need a modern approach to managing their digital ecosystem which recognizes the ubiquitous nature of Information Technology ("IT") in all aspects of internal and external court operations. There is a need for strategic, efficient, and highly responsive management and systems to address all the evolving challenges inherent in the digital world.

We believe OCA can build upon the existing foundation of their IT staff to meet these challenges by reorganizing and reassigning various leadership responsibilities, including designating a Chief Information Officer ("CIO") reporting directly to the Chief Administrative Judge ("CAJ"), which would not only accord with industry best practices, but will institutionalize the realities of operating in parallel physical and digital ecosystems. Such change will need little additional staff but will require a shift in thinking that elevates and fully appreciates the distinct nature of court digital operations in concert with traditional physical management concerns.

EXECUTIVE SUMMARY

It is the Working Group's recommendation that the Department of Technology ("DT") be rearranged and tasks reassigned in accord with industry best practices, including shifting the Director of Technology to a CIO position to whom four high-level managers report on the key operational areas of Technology, Security,[1] Project Management, and Network Infrastructure and Support. The CIO, in turn, would be included in the CAJ's executive team, thereby weaving the Court's digital operations into the overall day-to-day management of OCA's work, including aspects of strategic planning and incident preparedness, and to elevate the digital ecosystem to parallel the court's operations in the physical world.

1 OCA's General Counsel maintains responsibility for data privacy and legal compliance issues, serving as a *de facto* Chief Privacy Officer, while relying on DT leadership to protect the security of OCA's electronic storage and systems.

This report begins with a discussion of the current DT structure, and then highlights several key forward-thinking and strategic duties of the CIO. We then proceed to discuss opportunities to reorganize and align OCA's current IT management to accord with industry best practices, and to identify important strategies to achieve continued assessment and improvement with the evolving challenges in managing the court's digital ecosystem. Finally, we address several examples of modern IT management from New York State, the federal courts system, and he financial services industry as well as broader industry guidance.

I. Recommendations for Improving OCA's Digital Operations

A. Restructuring of DT

OCA's DT is capable of managing one of the most expansive digital operations among any state judiciary. With some adjustments to DT's current management structure and reassignment of supervisory tasks, including separating management into four key areas of Technology, Security, Project Management, and Network Infrastructure and Support, the Working Group believes OCA will significantly increase efficiency and strategic planning in its digital operations, and will provide the CAJ better oversight and governance of the court's entire digital footprint, while enhancing both the CAJ's and OCA's overall responsiveness in emergency situations. A current organizational chart is attached as **Exhibit A**, while a proposed reorganization is attached as **Exhibit B**.

The DT employs approximately 350 professionals within four key operational areas of Technology, Security, Project Management, and Network Infrastructure and Support; however, as each area has grown over time, so too has a strata of approximately 20 managers reporting directly to a single Director of Technology. (*See* **Exhibit A**). Many of these 20 managers often focus on more granular operational issues requiring day-to-day monitoring, with less room for big picture, strategic planning. In turn, the Director of Technology engages with these managers often on the granular issues within their purview, again often focusing on the day-to-day operational issues of ongoing system management. As 2020 has demonstrated, when faced with unexpected challenges such as the current health crisis impacting physical operations, the DT cannot afford to have its broad horizontal operational structure interfere with its ability to plan for contingencies.

Restructuring must begin with repositioning the current Director of Technology into the role of CIO to oversee all aspects of court operations in the digital ecosystem. In turn, the current 20 managers responsible for somewhat granular day-to-day operations would have positioned above them four (4) direct, high-level management individuals taken from existing managers, each overseeing a key areas of Technology, Security, Project Management and Network Infrastructure and Support. (*See* **Exhibit B**.) The CIO, as in most modern organizations, would report directly to the CAJ regarding the court's entire electronic footprint, as a parallel to the Court's operations in the physical space.

B. Improvements Resulting from the Reorganization

First, the proposed restructuring would expand the distance between the CIO and management of day-to-day operations, which then increases the CIO's time and resources available for strategic enterprise planning, focused and streamlined DT management, improved internal and external messaging, and enhanced preparations for incident response. The key, in our opinion, is to provide such person the freedom to focus on long-term goals and strategies in collaboration with the CAJ, freed from day-to-day tasks, and then to distribute supervision of key operating areas among four high-level managers better able to foster internal efficiencies, cooperation and employee engagement. We highlight the following critical CIO responsibilities intended to replace these day-to-day operational concerns. Attached as **Exhibit C** are helpful examples of job descriptions illustrating these key areas, including the Illinois Judicial Management Information Services Division Chief Information Officer and Michigan Third Judicial District Chief Information Officer.

1. Executive-Level Visibility to the UCS Employees

Organizations often ignore the fundamentals and nuances of IT at their peril even though it is a significant operating expense, and organizations literally can no longer operate if IT systems and processes do not function. If our courts intend to fulfill their needs to our citizenry, the CIO needs to serve as a vital tool for the CAJ to incorporate IT issues throughout the management of the UCS in parallel with traditional physical operations not just as needed, but at a fundamental level on a day-to-day basis on par with physical resources.

2. Digital Strategic Planning

While the efforts of this Working Group will help the courts in the coming months and years, these efforts must be incorporated into the court's ongoing operations and the duties of the CIO. The functions of this Technology Working Group, including surveys, reports and long-term recommendations, should be themselves the regular and routine functions of an executive-level OCA employee, and, ideally, result in regular reports to educate, assist and engage the CAJ, akin to the mandatory five-year strategic reporting provided in the federal court system (*see* **Exhibit D**). Such planning should not only encompass worst-case scenarios presented by cyberattacks and public health crises but must consider the rapidly evolving IT landscape with an eye to continual improvement.

3. Preparedness and Incident Response

It is critical for an organization to have a single executive-team member responsible for all aspects of cybersecurity and data privacy, and for that individual to have direct access to the CAJ not merely when a problem arises, but as part of day-to-day operations sufficient to cultivate an organization-wide, top-down culture of cyber- and data-hygiene.

4. Virtual-State-Wide Leadership

Both within the DT, as well as to the broader state-wide Judiciary and general public, a CIO would serve as the "face" of the court's "digital life" for purposes of judicial and public education, internal customer support, communications, surveys, and staff management in parallel with traditional concerns. This leadership image is then distilled to all DT employees through the four high-level managers described below, encouraging more robust and constructive collaborations, and ongoing system improvements.

5. Liaison Role

New York's Courts need a voice to advocate for ongoing improvements to the IT posture both among judges and employees within UCS and OCA and also among the State's citizens, litigants and attorneys and Executive and Legislative branches and out across other court systems and technology groups spanning the United States.

Second, the reduction to four (4) high-level managers overseeing the fundamental operational areas of Technology, Security, Project Management, and Network Infrastructure and Support would allow for a modern organization that increases the opportunities for critical internal review and strategic planning within those areas, strengthening relationships among managers and direct reports and allowing for ongoing collaboration and employee engagement on a day-to-day basis. Stated simply, a single CIO with responsibility for overall operations, forecasting and budgeting would find it difficult to find the time to manage 20 direct reports across a wide horizon of technical and oftentimes quite granular issues. This restructuring and reassigning responsibility among four (4) high-level managers would allow for increased attention to and planning in discrete operational areas.[2]

Chief Technology Officer: Responsible for overall architecture of OCA's digital footprint, including operation of the Court's private telecommunications network across New York State, and countless local networks at hundreds of courthouses and offices servicing tens of thousands of computer devices and employees.

Chief Information Security Officer: Responsible for all aspects of system security architecture, asset management, cyber threat detection, data privacy, and employee training and monitoring on pace with the ever-expanding threat landscape.

Director of Network Infrastructure and Support: Responsible for managing the hundreds of thousands of individual computer devices deployed across the Court's entire digital footprint, from servers and routers to printers and monitors, along with device and network standards, as well as managing the Help Desk to assist over 50,000 end users.

Director of Project Management: Responsible for developing and implementing all Information Technology projects and improvements based on the needs of Technology, Information Security and Network Infrastructure.

A third benefit would be a fundamental reorientation of court management to elevate the importance of the court's digital operations on par with the court's traditional work in the physical world. The events of 2020 have clearly shown that our courts operate in the dual spheres of digital and physical, and that not being able to incorporate digital operations in daily management may interfere proper preparation for unforeseen events. Including a CIO into the CAJ's direct reports will necessarily help weave the growing number of IT considerations into the CAJ's decision-making process. Again, IT is no longer a matter of managing internal printers and workstations but encompasses an entire ecosystem in which the court operates. As such, IT issues cannot be managed through a director level manager but must be presented directly to the CAJ as an integral element woven into the fabric of court operations.

2 As stated above, the area of data privacy falls under the management of OCA's Office of Counsel, in line with Counsel's overall responsibility for legal compliance. Counsel, in turn, relies on the DT, including the information security officer, to safeguard the electronic systems hosting sensitive data.

A last benefit of restructuring is to mirror current industry standards, and to facilitate better interaction with external organizations. While seemingly minor, the DT utilizes a largely antiquated series of titles predicted on managing various technological systems and has not kept in line with modern titles reflecting a streamlined and forward-thinking IT posture. In plain terms, New York is better represented by a CIO overseeing a CISO, CTO, Director of Project Management and Director of Network Infrastructure, who in turn supervise the various managers with task-specific titles.

As part of the proposed restructuring in anticipation of the court's increased need to generate and to manage digital content across a new public-facing website, social media and communication channels, OCA will need a C-level manager, generally known as a Chief Digital Officer ("CDO"), identified in the yellow cloud on the proposed reorganization chart (Exhibit B). Where, however, such an individual fits among OCA's larger structure is up to OCA. The responsibilities of this position depend in part on technology, but it more broadly may fall within the area of marketing and messaging. As such, the Working Group would recommend that OCA, at the appropriate time, strongly consider the addition of a CDO with control over the court's messaging across the digital ecosystem potentially within DT, though it is likely best situated elsewhere.

II. Examples of Executive-Level Information Technology Management

No longer is "Information Technology" limited to internal networks of workstations, printers, and servers, but it encompasses a standalone ecosystem touching on all aspects of digital operations. Current industry best practices underscore the need for an equally distinct operational structure with robust executive-level leadership responsible for all aspects of digital strategic planning, budgeting, and forecasting, and creating a direct reporting mechanism to chief executive management.

A. New York State Office of Information Technology Services ("ITS")

A helpful example of a robust IT management system is seen in New York's Executive branch. New York Technology Law §§ 102-103 affords the Office of Information Technology Services authority to establish all statewide technology policies and assigns administrative responsible for ITS operations to a CIO "in sole charge of the administration of the office" (id. §102[2]), who possesses exclusive authority to oversee, direct and coordinate the establishment of information technology policies, protocols, and standards for State government (Executive Order No. 117), including hardware, software, security and business re-engineering. The forward-thinking responsibilities of the CIO and, more broadly, ITS are many (Technology Law § 103), including the following three critical areas of strategic planning:

> (12) To complete a comprehensive study of existing state information resource technology infrastructure to the extent that the information is available. Such study shall include, but not be limited to, inventories of:
>
> (a.) state operations' computer hardware and software;
>
> (b.) major physical infrastructures supporting existing operations, including power, air conditioning, space and other environmental needs;

(c.) the telecommunications and other networks supporting existing operations;

(d.) personnel associated with existing operations and management;

(e.) expected retirement schedule of existing computer hardware and software and replacement costs; and

(f.) data processing consulting and contracting services utilized.

(12-a) To develop:

(a.) a methodology to ascertain how much the state spends on technology goods and services;

(b.) a process to update the computer hardware and software inventory periodically;

(c.) a methodology to determine the expected life-cycle of state operations' computer hardware and software which shall include the total cost of ownership; and

(d.) formal disaster recovery plans for the state data center and statewide network, NY e-net; such plans shall be confidential. Such developments shall be completed and submitted to the governor, the temporary president of the senate and the speaker of the assembly on or before October first, two thousand three.

(13) To establish a multi-year statewide strategy plan covering a time period of not less than three years to promote and coordinate interagency technology efforts and initiatives that conform to the state's overarching programmatic policy under which state agencies shall develop their information resource management plans….;

The CIO of ITS, responsible for assessing all proposals, is further guided by the following forward-thinking purposes:

- Promote innovation and deliver cost-effective IT solutions;
- Streamline the State's procurement and deployment of IT systems and infrastructure;
- Streamline the delivery of information or services by promoting consistency in handling, collecting, transporting, transferring, and storing of data;
- Promote short or long term cost savings by reducing duplication of spending and achieving greater economies of scale across State Information Technology Resources; and
- Create value for IT investments to better serve citizens, businesses, State Entities, and those who visit the State of New York websites.

(NYS IT Policy No: NYS-P08-002.)

B. Administrative Office of the United States Courts ("AO")

Another example of standalone IT leadership can be found in the federal courts' Office of Information Technology, which Office is independent of the Office of Management and Operations and Office Human Resources (*see* Org Chart, **Exhibit E**). In turn, the Office of Information Technology is broken into seven (7) separate departments, including:

- Computer Security and Independent Testing;
- Customer Relations;
- Technology Enhancement;
- Technology Policy, Planning, and Acquisitions;
- Applications Management and Development;
- Networks and Systems Integration; and
- Technology Training and Support.

In the Long Range Plan for Information Technology in the Federal Judiciary for fiscal years 2021 through 2025, the ubiquitous nature of technology in internal and external court operations is outlined in four elements:

- Public-facing technologies that serve the general public, as well as litigants, attorneys, law enforcement agencies, state and local courts, executive branch agencies, and other stakeholders
- Internal Judiciary systems used by judges and chambers, court staff, probation and pretrial services officers, and AO personnel.
- The technical infrastructure that is the underlying framework supporting the delivery and processing of information for all stakeholders, both internal and external. It includes the physical equipment, policies, and programs that ensure the quality and reliability of the Judiciary's IT services.
- IT security methods and processes that protect internal and external Judiciary systems, services, and data against unauthorized use, disclosure, modification, damage, inaccessibility, and loss.

(Attached as **Exhibit D**.)

C. National Institute of Standards and Technology Cybersecurity Framework

The Framework for Improving Critical Infrastructure Cybersecurity (version 1.1, April 16, 2018; attached as **Exhibit F**) provides another helpful explanation of the need for executive-level participation from a data privacy and cybersecurity prospective.

1.1 Overview of the Framework:

Framework Core: The Core presents industry standards, guidelines, and practices in a manner that allows for **communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level**.

2.2 Framework Implementation Tiers:

***

The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. **Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.**

***

The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. **Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks**.

2.4 Coordination of Framework Implementation:

Figure 2 describes a common flow of information and decisions at the following levels within an organization:

- Executive
- Business/Process
- Implementation/Operations

The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into the risk management process, and then collaborates with the implementation/operations level to communicate business needs and create a Profile. The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process and to the implementation/operations level for awareness of business impact.

D. Financial Services Industry

Both state and federal laws and regulations regarding cybersecurity and data privacy in the financial services industry provide helpful insights into the need for executive-level IT professional(s), not only to plan and prepare for potential data incidents, but also to serve as the agent with ultimate responsibility for maintaining and improving written policies and procedures. New York's Department of Financial Services regulations can be found at 23 NYCRR Part 500, while the Federal Trade Commission's Safeguards Rule, pursuant to the Gramm–Leach–Bliley Act (15 U.S.C. §§ 6801-6809), can be found at 16 CFR Part 314.

Under both sets of rules, entities are obligated to maintain clear standards relating to administrative, technical and physical safeguards that ensure the security and confidentiality of all personal information within their control, protect against any anticipated threats or hazards to the security or integrity of that information, and protect against unauthorized access or use of such information. 16 CFR § 314.3, 23 NYCRR 500.2. In New York, known as a Cybersecurity Program, while known as an Information Security Plan by the FTC.

A critical component in New York is the filing of a Certification of Compliance by someone on the organization's board of directors or senior officer, codifying the industry practice of including an IT manager at the executive level. 23 NYCRR 500.17(b). In the federal scheme, each organization must identify a person responsible for all security issues, and to prepare a written Information Security Plan to be reviewed and reassessed by leadership on a regular basis. 16 CFR §§ 314.3, 314.4.

Importantly, a proper Cybersecurity Program or Information Security Plan incorporates not only technical and physical safeguards, but also includes administrative protocols and comprehensive training elements, which would require coordination between an IT department and other operational units, including Human Resources. As such, in addition to executive participation in overall cybersecurity, there should be executive-level IT management staff on par with human resources or other departments to foster coordination and efficiency, and to realize that cybersecurity and data privacy are foundational aspects of modern enterprise.

TECHNOLOGY WORKING GROUP

THE TECHNOLOGY WORKING GROUP IS COMPOSED OF:

Working Group Chairs:

Mark A. Berman, *(Co-Chair)*, Partner, Ganfer Shore Leeds & Zauderer LLP

Sharon M. Porcellio *(Co-Chair)*, Member, Bond, Schoeneck & King, PLLC

Working Group Members:

Robert J. Ambrogi, *Partner, Journalist, Media Consultant and Blogger*, Law Offices of Robert J. Ambrogi and Law Sites Blog and LawNext Podcast

Michael DeVito, *Manager, Office of Record Production*, Office of Court Administration Division of Professional and Court Services

Hon. David Otis Fuller, *Village Justice of Tuckahoe*, Partner, Bosworth, Gray & Fuller and Past President, New York State Magistrate's Association

Maura R. Grossman, *Research Professor and Principal*, University of Waterloo and Maura Grossman Law

Scott L. Malouf, *Partner*, Law Offices of Scott L. Malouf

Mary C. McQueen, *President*, National Center for State Courts

Jack Newton, *Chief Executive Officer*, Clio

James M. Paulino II, *Partner*, Goldberg Segalla

Jeroen Plink, *Chief Executive Officer*, Clifford Chance Applied Solutions

Edward A. Steinberg, *Partner*, Leav & Steinberg, LLP

Patrick Turner, *Vice President, Associate General Counsel*, CBS Corporation

Ari Ezra Waldman, *Professor of Law and Computer Science*, Northeastern University School of Law and Khoury College of Computer Science

REIMAGINING OCA'S DIVISION OF TECHNOLOGY

A STRATEGIC REORGANIZATION

MEMBERS OF THE COMMISSION

Hon. Rolando T. Acosta
Hon. Ariel E. Belen
Mark A. Berman
T. Andrew Brown
Hon. Anthony Cannataro
Mylan L. Denerstein
Hon. Craig J. Doran
Richard A. Edlin
Hon. Michael J. Garcia
Robert J. Giuffra, Jr.
Dennis E. Glazer
Alecia Walters-Hinds
Hon. Timothy C. Idoni
Seymour James
Brad S. Karp
Roger Juan Maldonado
Hon. Edwina G. Mendelson
Jack Newton
Sharon M. Porcellio
Paul C. Saunders
Arthur J. Semetis
Paul Shechtman
Michael A. Simons
Hon. Madeline Singas
Hon. Leslie E. Stein
Edward A. Steinberg
Ari Ezra Waldman

Produced by the Technology Working Group of the
Commission to Reimagine the Future of New York's Courts.

NYS Office of Court Administration
Division of Technology and Court Research
Organization Chart
November, 2020

Application Development

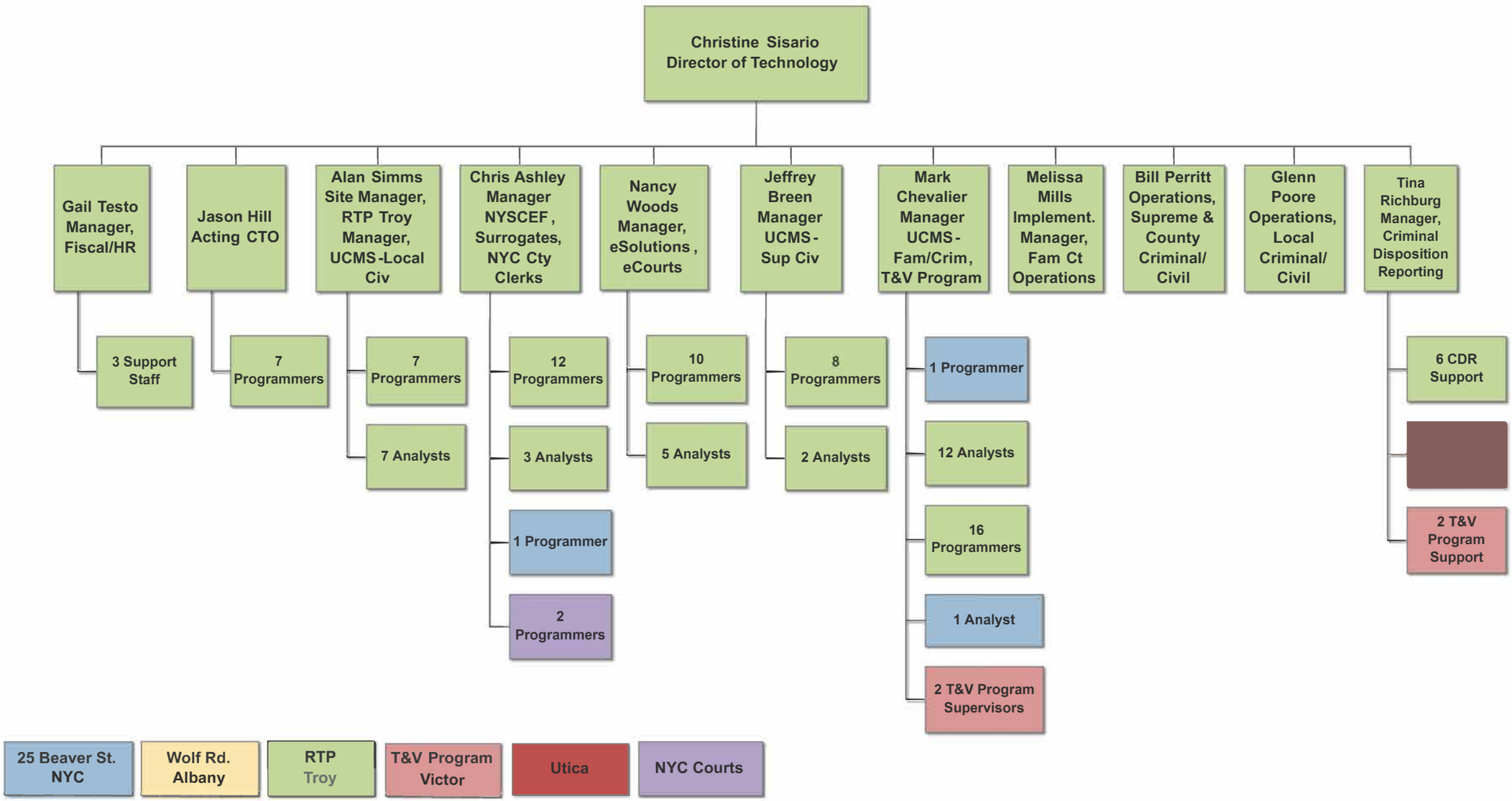


EXHIBIT | A1

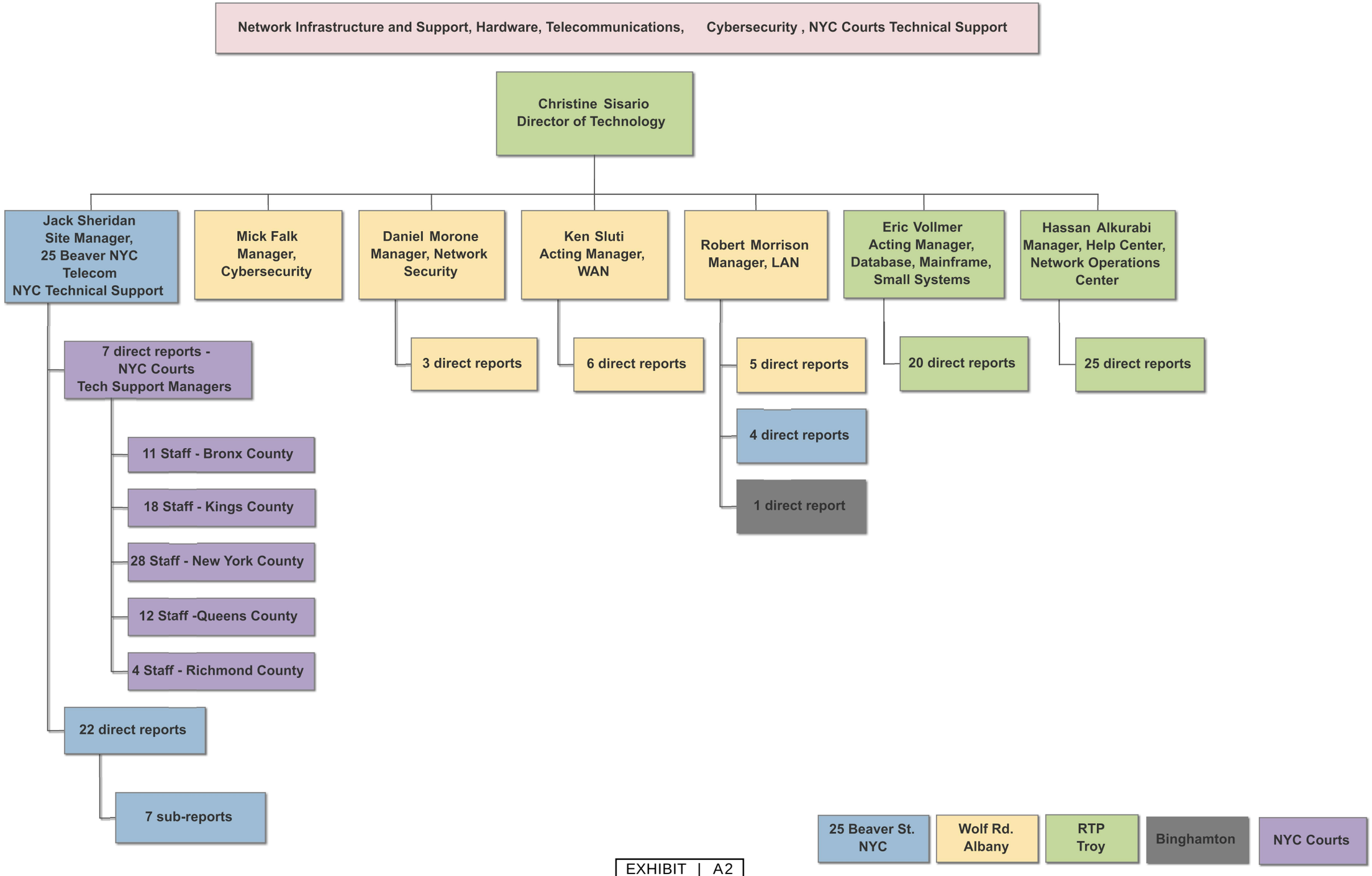

Network Infrastructure and Support, Hardware, Telecommunications, Cybersecurity , NYC Courts Technical Support
Christine Sisario
Director of Technology
Jack Sheridan
Site Manager,
25 Beaver NYC
Telecom
NYC Technical Support
Mick Falk
Manager,
Cybersecurity
Daniel Morone
Manager, Network
Security
Ken Sluti
Acting Manager,
WAN
Robert Morrison
Manager, LAN
Eric Vollmer
Acting Manager,
Database, Mainframe,
Small Systems
Hassan Alkurabi
Manager, Help Center,
Network Operations
Center
7 direct reports -
NYC Courts
Tech Support Managers
11 Staff - Bronx County
18 Staff - Kings County
28 Staff - New York County
12 Staff -Queens County
4 Staff - Richmond County
22 direct reports
7 sub-reports
3 direct reports
6 direct reports
5 direct reports
4 direct reports
1 direct report
20 direct reports
25 direct reports
25 Beaver St.
NYC
Wolf Rd.
Albany
RTP
Troy
Binghamton
NYC Courts

EXHIBIT | A2

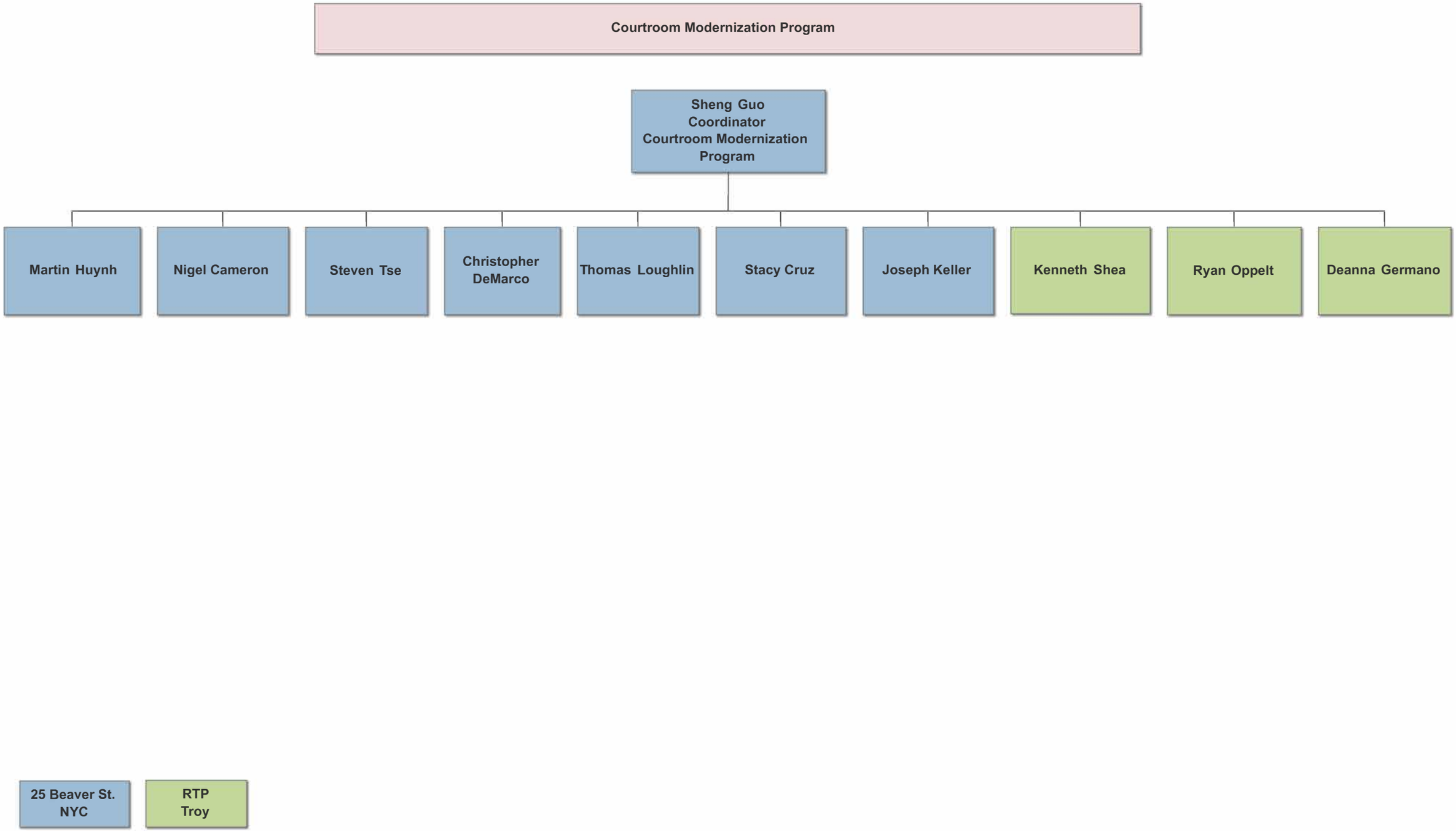
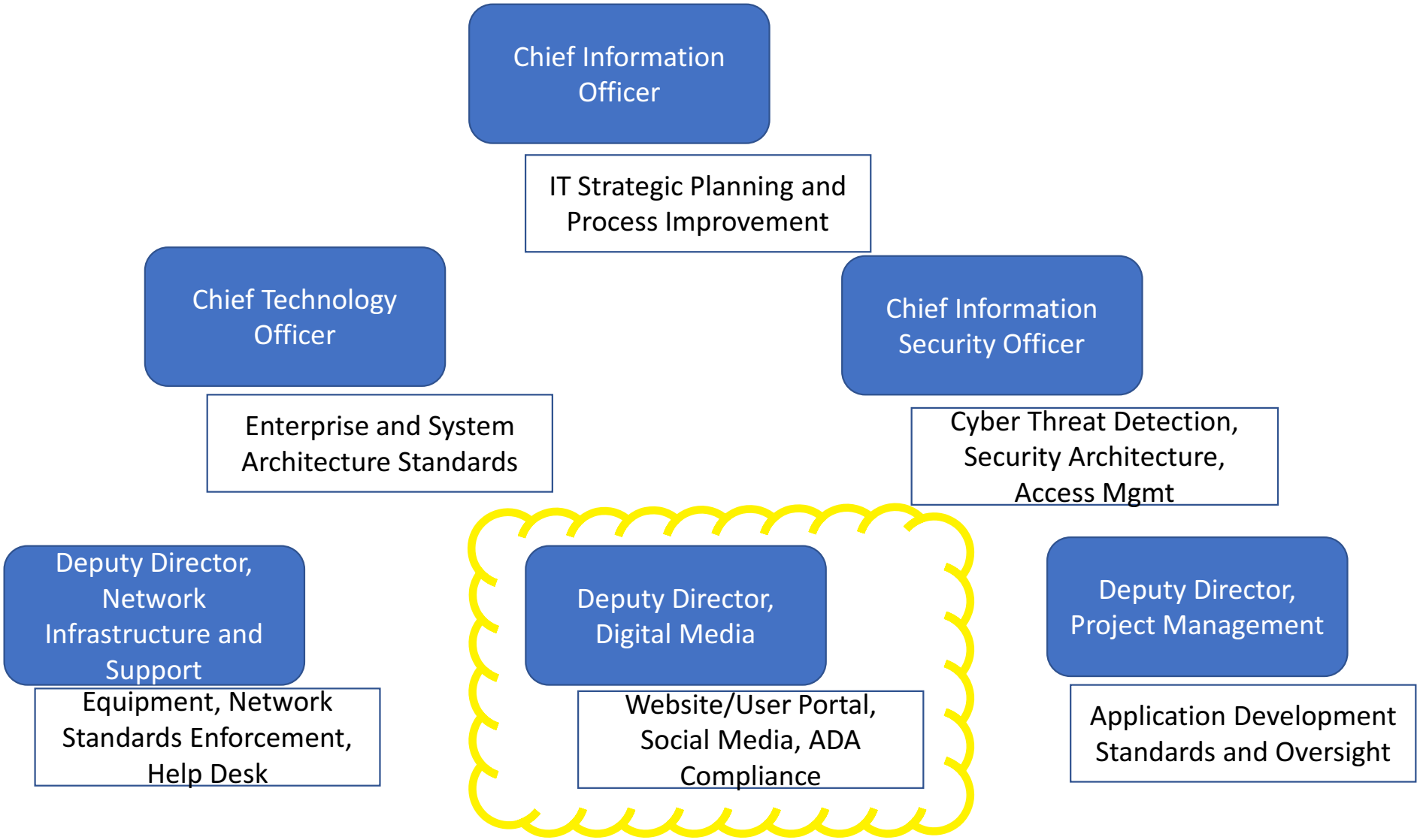

Courtroom Modernization Program
Sheng Guo
Coordinator
Courtroom Modernization
Program
Martin Huynh
Nigel Cameron
Steven Tse
Christopher
DeMarco
Thomas Loughlin
Stacy Cruz
Joseph Keller
Kenneth Shea
Ryan Oppelt
Deanna Germano
25 Beaver St.
NYC
RTP
Troy

EXHIBIT | A3


Chief Information Officer
IT Strategic Planning and Process Improvement
Chief Technology Officer
Enterprise and System Architecture Standards
Chief Information Security Officer
Cyber Threat Detection, Security Architecture, Access Mgmt
Deputy Director, Network Infrastructure and Support
Equipment, Network Standards Enforcement, Help Desk
Deputy Director, Digital Media
Website/User Portal, Social Media, ADA Compliance
Deputy Director, Project Management
Application Development Standards and Oversight

Third Judicial Circuit of Michigan
Office of Human Resources

Classification Code: 0400-0002 **Date Issued: 01/17/2013**

TITLE: **CHIEF INFORMATION OFFICER**

SUMMARY:

Is responsible for all of the Court's technological needs including the development, maintenance, and support of its core IT infrastructure, enterprise and department specific applications, and court-wide applications and programs including case management and e-filing systems. Sets the Court's overall direction for technology through strategic planning and evaluation. Provides leadership, planning and management for all areas of information technology strategy, development, implementation and support necessary for efficient operation of the Court and to achieve long-range goals. Reports to the Executive Court Administrator. Employees in this title are expected to maintain a professional appearance and demeanor.

ESSENTIAL FUNCTIONS:

- Contributes to general business planning regarding technology and systems required to maintain and promote Court operations.
- Evaluates overall information technology operations.
- Oversees the design and implementation of new applications and changes to existing systems and software.
- Evaluates and procures new hardware and software to meet Court needs.
- Reviews, approves and negotiates vendor proposals and contracts for all new technology purchased for the Court.
- Ensures the development and implementation of cost-effective systems and efficient computer operations to meet current and future requirements.
- Consults with administration, managers and industry representatives to exchange information, present new approaches and to discuss equipment/system changes.
- Recognizes new developments in information systems technology and anticipates organizational modification needs.
- Establishes long-term needs for information systems, plans strategy for developing systems and acquiring hardware to meet application needs.
- Oversees management of present information systems, and directs staff for efficient operation and for prompt modernization and upgrades as needs of the Court change.
- Ensures confidentiality and reliability of corporate data, proprietary information, and intellectual property.
- Functions as the top-level contact to assist end-users in determining information systems requirements and solutions.
- Keeps abreast of government regulations applicable to systems operations and ensures corporate compliance.
- Builds strong relationships and serves as the Court's liaison to external local, regional and national governmental and regulatory agencies relative to technology planning and issues. Consults with and/or forms plans with SCAO and other courts on issues of mutual interest related to information technology.
- Performs other duties as assigned.

Third Judicial Circuit of Michigan
Office of Human Resources

Classification Code: 0400-0002 **Date Issued: 01/17/2013**

TITLE: **CHIEF INFORMATION OFFICER**

QUALIFICATIONS:

- Bachelor's degree in Computer Science, Information Technology, Business Administration, Public Administration or related field. Master's degree preferred.
- Seven (7) years of increasingly responsible experience in administration of information systems and technology.
- Must possess (at time of application) and maintain a valid Michigan driver's license, no fault insurance and access to a vehicle to use in the performance of assigned duties.
- Knowledge of software applications, networking and data management strategies.
- Experience in areas of budgetary/fiscal management, and project management, including assessing risks and exposures, identifying options and alternatives, making decisions, and implementing corrective actions.
- Proficient using MS Office Suite and relevant software and systems.

KNOWLEDGE, SKILLS AND ABILITIES:

- Ability to manage complex technology projects from inception to completion.
- Skilled strategic and visionary thinker with excellent ability to conceptualize long-term business goals and develop an orderly process of planning to accomplish those goals.
- Excellent verbal, written, interpersonal, presentation, public speaking and meeting management communication skills.
- Ability to communicate and work with all stakeholders and departments.
- Demonstrated leadership and managerial skills.
- Ability to simultaneously coordinate multiple projects and complex tasks while meeting deadlines.
- Strong business acumen and a solid foundation in information technology, including change management and project management experience.
- Knowledge of software applications, networking and data management strategies.
- Ability to apply innovative thinking in conjunction with technical understanding of emerging technologies to address needs relative to providing services to the Court.
- Ability to review and modify business processes to meet the ever changing needs of a complex and dynamic environment.
- Knowledge of the principles, practices and procedures of management and administration.
- Ability to remain calm and use good judgment in difficult situations.
- Ability to establish and maintain effective working relationships with coworkers, employees, officials and external contacts.
- Ability to simultaneously coordinate multiple projects and complex tasks while meeting deadlines.
- Skill in managing one's own time and the time of others, as well as the ability to meet deadlines.
- Skill in training, counseling employees and interacting tactfully.
- Thorough knowledge of Court processes and procedures.

Third Judicial Circuit of Michigan
Office of Human Resources

Classification Code: 0400-0002 **Date Issued: 01/17/2013**

TITLE: **CHIEF INFORMATION OFFICER**

WORK ENVIRONMENT:

- Normally a typical customer service office environment with minimal exposure to excessive noise.
- Employees in this title may encounter individuals who may be under duress.

PHYSICAL REQUIREMENTS:

- Sitting at desk for long periods of time to perform job functions.
- Ability to read, write and interpret written documents.
- Use hands to manipulate, handle, feel, and control items or equipment.
- Walk, bend, reach, stand and sit.
- Talk, hear, and communicate with clients, co-workers, and others.
- Ability to operate a motor vehicle.

LICENSES, CERTIFICATIONS OR SPECIAL REQUIREMENTS:

- Candidates considered for placement in this job title will be subject to a criminal background investigation and subsequent fingerprinting every five years.
- Must possess (at time of application) and maintain a valid Michigan driver's license, no fault insurance and access to a vehicle to use in the performance of assigned duties.

The above statements describe the general nature and level of work performed by employees assigned to the title. Incumbents may be required to perform job-related responsibilities and tasks other than those stated in this description. Specific job duties vary from position to position.

NOTES:

1/17/2013 Title added
11/17/2017 Updated for content and format

Administrative Office of Illinois Courts
Chief Information Officer

PURPOSE

Directs the planning and implementation of enterprise IT systems for the Information Technology Services.

ESSENTIAL FUNCTIONS

- Provides administrative, technical, and planning direction for the operation of the JMIS Division.
- Strategizes technological planning to achieve business goals by prioritizing technology initiatives and coordinating the evaluation, deployment, and management of current and future technologies.
- Provide executive leadership and technical direction to plan, direct, and execute IT operations, information security, and enterprise architecture.
- Collaborates with other division directors, judges, and Department leaders to develop and maintain a technology plan that supports the Department's needs.
- Reviews hardware and software acquisition and maintenance contracts, and pursues master agreements for products and services on an enterprise scale.
- Represents ITS on inter-governmental projects; promote and oversee strategic relationships with and external entities, including other state and local agencies, vendors, and partner organizations.
- Conducts research to remain knowledgeable of industry trends and emerging technologies to support new initiatives, opportunities, and information security best practices.
- Consults with the Administrative Director to define the parameters and priorities of current and future projects, to determine processing requirements, to meet current and future informational needs, and to determine the equipment capabilities necessary to meet these requirements; apprises the Administrative Director of staff activities and status of projects.
- Evaluates and recommends personnel staffing requirements and hiring, equipment and budgetary needs; establishes work standards, policies, and procedures; authorizes JMIS expenditure requests, including EDP equipment and software applications, contractual obligations, and travel.
- Directs the statewide operations and coordination of data processing, software applications, telecommunications, and other informational needs for the judicial branch.
- Analyzes data requirements and flow to recommend project reorganization or realignment.
- Prepares agenda items as directed by the Administrative Director.
- Manages the Court's website.

- Manages security and security related issues for information systems of the judicial branch.
- Prepares and submits progress reports of Division activities upon request or as required.
- Performs other duties as assigned.

EXPERIENCE AND EDUCATION REQUIREMENTS

Bachelor's degree in a related field and five years of related work experience; or an equivalent combination of education and experience.

Requires a driver's license, proof of valid automobile insurance when operating a personal vehicle on state business, and a safe driving record.

SELECTION FACTORS

KNOWLEDGE AND SKILLS

1. Knowledge of the Judicial Branch including data requirements of a judicial information system.
2. Knowledge of information systems, data processing procedures, and the principles and practices of quantifying techniques.
3. Knowledge of computer hardware, software, and peripheral equipment.
4. Skills in program development, implementation, and evaluation.
5. Working knowledge of Microsoft Word, PowerPoint, Excel, and Access and/or other applications utilized by the judicial branch.
6. Knowledge of the principles and techniques of short-term and long-range project management.
7. Strong written and oral communication skills.
8. Strong organizational and interpersonal skills.
9. Use of independent judgment within established practice and procedural guidelines.
10. Knowledge of and ability to use supervisory principles and practices, including work prioritization and scheduling, employee motivation, and performance evaluations.

PHYSICAL REQUIREMENTS

1. Ability to sit for extended time periods.
2. Normal office working environment requiring telephone usage and ability to process written documents.
3. Travel within state required

Fiscal Year 2021 Update

Long Range Plan for Information Technology in the Federal Judiciary

Approved by the Judicial Conference of the United States

September 2020

EXHIBIT | D1

Contents

Introduction

2021

The *Strategic Plan for the Federal Judiciary*[1] defines the Judiciary's mission as follows:

> *The United States Courts are an independent, national Judiciary providing fair and impartial justice within the jurisdiction conferred by the Constitution and Congress. As an equal branch of government, the federal Judiciary preserves and enhances its core values as the courts meet changing national and local needs.*

Judges and Judiciary staff regard information technology (IT) not as something separate from their day-to-day work, but as a means by which they do their jobs. As business processes and technology solutions have become interwoven, the Judiciary recognizes that IT presents opportunities not simply to replicate old paper processes in digital form but to reengineer many aspects of those processes altogether.

Pursuant to section 612 of Title 28, United States Code, the Director of the Administrative Office of the United States Courts (AO) is responsible for preparing and annually revising the *Long Range Plan for Information Technology in the Federal Judiciary* (*Long Range Plan*). The Committee on Information Technology of the Judicial Conference of the United States provides guidance in the development of annual updates and recommends the plan for approval by the Judicial Conference. Upon approval, the Director provides the annual update of this plan to Congress.

This update to the *Long Range Plan* describes key strategic priorities for the IT program over the next three to five years, and summarizes the Judiciary's anticipated IT resource requirements for fiscal years (FY) 2021 through 2025. The strategic priorities discussed in this document integrate the *Strategic Plan for the Federal Judiciary*, as updated in 2015, with the IT planning and budgeting process and Judiciary-wide strategic planning efforts. The strategic priorities were further informed by discussions within the AO's advisory process, as well as circuit judicial and IT conferences.

The Judiciary's IT program consists of systems and services provided both at the national level and by the courts individually. The program consists of four elements:

- Public-facing technologies that serve the general public, as well as litigants, attorneys, law enforcement agencies, state and local courts, executive branch agencies, and other stakeholders.
- Internal Judiciary systems used by judges and chambers, court staff, probation and pretrial services officers, and AO personnel.
- The technical infrastructure that is the underlying framework supporting the delivery and processing of information for all stakeholders, both internal and external. It includes the physical equipment, policies, and programs that ensure the quality and reliability of the Judiciary's IT services.
- IT security methods and processes that protect internal and external Judiciary systems, services, and data against unauthorized use, disclosure, modification, damage, inaccessibility, and loss.

[1] *Strategic Plan for the Federal Judiciary*, approved by the Judicial Conference of the United States, September 2015.

Strategic Priorities

The *Strategic Plan for the Federal Judiciary* includes the strategy, "Harness the potential of technology to identify and meet the needs of court users and the public for information service, and access to the courts," as well as four associated goals which form the basis of strategic priorities for IT:

- Continue to build and maintain robust and flexible technology systems and applications that anticipate and respond to the Judiciary's requirements for efficient communications, record-keeping, electronic case filing, case management, and administrative support.
- Coordinate and integrate national IT systems and applications from a Judiciary-wide perspective and more fully utilize local initiatives to improve services.
- Develop system-wide approaches to the utilization of technology to achieve enhanced performance and cost savings.
- Refine and update security practices to ensure the confidentiality, integrity, and availability of Judiciary-related records and information.

The following sections describe significant initiatives that are planned over the next three to five years to address each of these strategic priorities.

Continue to build and maintain robust and flexible technology systems and applications that anticipate and respond to the Judiciary's requirements for efficient communications, record-keeping, electronic case filing, case management, and administrative support.

IT is inextricably part of the performance of the Judiciary's business. Applications to perform case filing, case management, and administrative support are supported by communications and collaboration systems. These systems and applications require ongoing maintenance, improvement, upgrades, and replacement in order to remain functional in a continually changing external environment as well as relevant to the current needs of the Judiciary. In addition to managing a structured lifecycle-management process to identify, manage, and implement user requests for system improvements, the Judiciary regularly assesses whether business needs or new technologies necessitate more extensive upgrades or even replacement of systems.

Descriptions of anticipated system and application changes are provided as examples of this planning process in action and to delineate the areas on which the Judiciary will place priority over the next three to five years.

Electronic Public Access

The Judiciary provides electronic access to case information, including the documents in case files, through its Public Access to Court Electronic Records (PACER) System. The public and other external stakeholders do not need to visit courts in person to obtain a case file and photocopy documents. Instead, the program's three million registered users can obtain these documents and other case information online. At the same time, to strengthen security and protect privacy, the Judiciary has instituted policies that restrict access to certain types of cases, information, and documents.

The Judiciary's Electronic Public Access (EPA) program established a Public User Group to provide advice and feedback on ways to improve PACER and other electronic public access services provided by the Judiciary. The EPA program is also redesigning the PACER.gov website. Progress in updating the public-facing applications accessible from the PACER website continues to provide a more consistent and unified user experience in the areas of authentication, billing, and account management.

Case Filing/Case Management

The federal courts case filing process is managed by the Case Management/Electronic Case Files (CM/ECF) System, through which attorneys open cases and file documents over the internet. Case information and related documents are electronically available to case participants at virtually the same moment a filing is completed. Nearly instantaneous email notification of any activity in a case maximizes the time available for participants to respond. These efficiencies have reduced the time and cost required for litigants to work through the judicial process. The public benefits from electronic case file document availability through the PACER system as a result of the CM/ECF filing process.

EXHIBIT | D5

The implementation of Next Generation CM/ECF (NextGen) modernizes the business processes used by the courts and judges' chambers. NextGen enhances the way judges manage case information, providing the information they need to work with minimal additional effort. NextGen also enables judges, court staff, and attorneys to access CM/ECF data in multiple courts using a single account; provides appellate attorney filers with a new, streamlined interface; enhances the Judiciary's ability to exchange data within its internal systems and between internal and external systems; supports a more consistent user experience for external users of the case management system; improves filing capabilities for pro se filers in bankruptcy cases; and provides a new, streamlined interface for automatic judge and trustee assignments in bankruptcy cases.

All appellate courts are live on NextGen CM/ECF. Implementation waves for district and bankruptcy courts began in January 2018, and quarterly implementation waves, with 15 courts in each, began in July 2018. By 2021, the last wave of courts is anticipated to begin the implementation process to migrate to NextGen CM/ECF.

There will be at least one new NextGen and one Current Generation CM/ECF (CurrentGen) release per year for each court type. The CurrentGen releases will implement security updates and address any necessary required changes (due to new rules, for example). The NextGen releases will also include the resolution of security vulnerabilities and bug fixes based on priorities established by court expert panels. Finally, enhancements and new functionality may be delivered if required by new laws or direction from the Judicial Conference.

The Probation and Pretrial Case Tracking System, also known as PACTS, has evolved into a comprehensive case management system for probation and pretrial services officers, and has become an indispensable supervision and investigation tool. In recent years, the IT applications maintained by the AO in support of the probation and pretrial services system have had significant problems with reliability and performance. To resolve these issues, the AO proposed a two-step plan to

ensure the reliability and performance of PACTS and the related applications. The first step is to stabilize PACTS and existing applications while a replacement system is developed and deployed. The second step is to develop a replacement system for PACTS, using commercial off-the-shelf (COTS) products as well as a highly configurable platform solution. The replacement system will continue to interface with key applications, both internal and external to the Judiciary, and provide officers the data necessary to fulfill their mission. Replacement is expected to be a multi-year project, with work completed in stages. Solicitation activities, including a data migration strategy, occurred in FY 2019. A vendor was selected in April 2020.

Jury Management

Jurors perform a vital role in the U.S. system of justice. Jury service is an important civic function that supports one of the most fundamental rights of individuals—the right to have the interests of justice reviewed and determined by fellow citizens. The Constitution provides that the "trial of all crimes, except in cases of impeachment, shall be by jury." U.S. Const. art. III, § 2, cl. 3. The right of the accused in criminal prosecutions to trial by jury is protected by the Sixth Amendment to the Constitution and the right to trial by jury in civil actions is preserved by the Seventh Amendment to the Constitution. The Judiciary must update its 20-year-old, Windows-based jury management system because it will soon become obsolete. It will be replaced with a web-based solution, which will be less expensive and easier to maintain and operate. The web-based solution will be centrally managed to allow for a quicker response to security findings and more regular technical enhancements. Business requirements have been documented and the next step will be to procure software that can be customized through a partnership between Judiciary experts and a vendor to meet the Judiciary's needs.

Judges and Chambers Staff

Although case management systems were originally designed primarily to manage documents and processes in the clerks' offices, NextGen CM/ECF is introducing efficiencies to judges' chambers. New features have been developed, such as the Judge Review Packet which provides district and bankruptcy judges and their staff with the ability to automatically create and maintain electronic packets of information for matters that require chamber's review and actions. Judges and their staff will also have the advantage of utilizing a user interface called Workspace, which provides customizable screen content based on job function. Mobile Briefcase allows appellate judges and their staff to download and edit documents on a tablet computer. The Citation Links functionality adds links to PDF documents filed in a case so that judges, law clerks, and court staff can easily view the referenced content using their preferred resources (e.g., LexisNexis, Westlaw). An integrated calendar for district and bankruptcy judges began as a proof of concept in 2018. The Calendar module, one of the most complex components of the new system with over 2,000 requirements defined by judges and court staff, is currently being piloted by one district court (N.D. Fla.) and three bankruptcy courts (Bankr. D. Alaska, Bankr. D.N.J., and Bankr. D. Or.). Testing of the Calendar module has been moving slowly, however, with delays in preparing and developing the software to allow the pilot courts to go live on the module. Considering these issues and others, it is uncertain whether the Calendar module will be released broadly.

Administrative Support

Several nationally deployed administrative systems supporting finance, human resources, and facilities management are in the midst of upgrade or replacement. The goal is to deliver high-quality, secure solutions aimed at reducing costs, enhancing the user experience, and strengthening internal controls.

Deployment of the Judiciary Integrated Financial Management System (JIFMS) has been completed, and it is now in use throughout the Judiciary supporting the core accounting and procurement functions. In May 2020, debt management functions in JIFMS will also be fully deployed nationwide. JIFMS provides enhanced interfaces with external systems, improved data sharing capabilities, improved internal controls, and standardized business practices.

EXHIBIT | D6

The AO is now positioned to upgrade the JIFMS product to the latest version. This upgrade will provide enhanced functionality, support for the latest infrastructure, and position the AO to deploy several government-wide solutions such as the Invoice Processing Platform (IPP)[2] and G-Invoicing[3] in the future. It will also resolve several known software defects. Once the upgrade is completed, a routine and predictable upgrade cycle will be established, allowing the Judiciary to take advantage of an up-to-date and supportable financial management solution into the future.

The AO will pursue a "back to baseline" strategy that involves minimizing Judiciary-specific customization of the underlying COTS software. Minimizing customization should result in streamlined operations and maintenance activities, reduced complexity of future upgrades, and help achieve the goal of establishing a routine and predictable upgrade cycle.

Development efforts are also underway for an Automated Collections Register (ACR) system to replace the various systems used by district, bankruptcy, and appellate courts. Currently, the cash register function is decentralized with a variety of different cash register solutions being used throughout the Judiciary. Many of the solutions being used today are obsolete and difficult to maintain due to aging technology. The development of the ACR system is another step to unify the Judiciary on a single platform, utilizing up-to-date software and infrastructure that can be supported nationwide. The solution is being designed to integrate with the Judiciary's financial and case management systems. With the court community leveraging a single system, the AO can further meet future legislative, business, and technological requirements.

Lastly, the AO is pursuing a unified debt management solution that will replace the Civil/Criminal Accounting Module, which is currently integrated into JIFMS and other debt management solutions used throughout the Judiciary. This solution will offer debt management functionality for the district and bankruptcy court community. Efforts are currently underway to identify and define key business processes. Once these are defined, requirements will be gathered, followed by development and implementation activities. The AO is actively engaging with the court community and the Financial Managers Working Group on this initiative.

Each of the efforts is designed to align with, and complement, a five-year Judiciary strategic effort called the Judiciary Data Integrity, Reporting and Controls (JDIRC) program, to produce annual financial statements for the Judiciary that are audited, and consolidated in a standardized way throughout the Judiciary. The JDIRC program will transform financial reporting requirements across the Judiciary, improve the Judiciary's internal controls programs, and strengthen the integrity of Judiciary financial data.

The Human Resources Management Information System (HRMIS) manages human resources transactions, including leave tracking, employee performance, and payroll production for the Judiciary. The AO is focused on making system improvements to address regulatory and statutory requirements driven by the executive and legislative branches. In addition, efforts are underway to enhance the utilization of the non-mandatory modules of HRMIS, Leave Tracking and ePerformance. Plans call for establishing communities of practice and focus groups to share information and gather feedback related to these products and make them attractive alternatives to local development or procurement efforts. Additional goals include improving training and communications about HRMIS.

Recognizing the importance of "people" data supporting other solutions and capabilities, the AO continues to explore opportunities to provide such data so that it can be used appropriately by other systems in accordance with Judiciary data governance principles.

Similar to the financial systems, the AO is focused on establishing a routine upgrade cycle for HRMIS to minimize the impact to the user community while optimizing new features and maintaining an up-to-date, supportable human resources management solution into the future.

In its continuing effort to improve and standardize the background check process outlined in the Guide to Judiciary Policy, Volume 12 (Human Resources), Chapter 5 (Employment), § 570 Background Checks and Investigations, the AO is pursuing a procurement for a new fingerprint solution that will standardize how all

[2] IPP is a web-based system that provides one integrated, secure system to simplify the management of vendor invoices.

[3] G-Invoicing is the long-term solutions for Federal Program Agencies to manage their intragovernmental Buy/Sell transactions; https://www.fiscal.treasury.gov/g-invoice/.

court units and Federal Public Defender Organizations (FPDOs) enter and transmit biometric information. The new solution will replace the current methods used to submit fingerprints for background checks (inked fingerprint cards and LiveScan fingerprints), increase the security of the data, and improve the efficiency of the overall process. Unlike the legacy solutions, the new centrally maintained, web-based solution will operate on a local computer with other applications (i.e. JIFMS, JENIE) rather than on a stand-alone machine. No data will be stored on the local device, which will protect personally identifiable information (PII), and all data will be securely transmitted to a central repository.

The Ethics in Government Act requires all judicial officers and certain Judiciary employees to file financial disclosure reports. A new system for this purpose is in development, leveraging the executive branch tool and enhancing the functionality to meet the needs of Judiciary filers and those administering the program. Deployment has shifted and will begin in late FY 2020, with full deployment of the first phase in FY 2022. This new system is part of the larger program that includes correspondence automation and tracking; release and redaction; and compliance for financial disclosure reports.

Efforts are underway to develop and implement a COTS real estate and facilities management system to replace disparate systems and tools used today. The new system, called JSPACE, will provide comprehensive data and analytics for the Judiciary to manage more than 30 million usable square feet of space in 850 locations with an annual rental cost of almost $1 billion. Furthermore, it will support the Judiciary's long-range facilities planning efforts and overall rent and space management function as well as the Capital Security Program and initiatives such as space reduction and service validation. Full deployment is anticipated by FY 2023.

The AO is committed to improving emergency communications within the Judiciary. A new Judiciary Disaster and Recovery Tool (JDART) initiative began this year to provide improved information for assessing and monitoring a wide range of threats to Judiciary facilities and personnel. Based on current geographic information system technology, the new tool will provide a single operational view of developing emergency situations, e.g., natural or man-made disasters, and help Judiciary decision-makers and emergency personnel quickly and effectively assess and respond to evolving situations. The AO will also explore additional solutions to strengthen communications and situational awareness during emergency situations.

A standard set of development and integration platforms are being adopted within the administrative support arena. The platforms include low code, robotic process automation (RPA) with artificial intelligence (AI), service bus for application programming interface (API) centric integration, business intelligence and workflow solutions. The goal is to leverage these tools to reduce historical custom code complexity and replace it with standards-based platforms that enhance security, improve quality, provide consumer-friendly user experiences, and reduce the time to market for administrative support products and services. The services and capabilities of these platforms will be incorporated in the service delivery model as the tools are adopted.

Coordinate and integrate national IT systems and applications from a Judiciary-wide perspective and more fully utilize local initiatives to improve services.

Coordinate and Integrate National IT Systems and Applications

The Judiciary manages a broad array of information in its suite of national systems. As in many organizations, these systems were developed separately over time to support various lines of business, such as case management and court administration, probation and pretrial services, human resources, and financial management. Although the systems were developed

separately, the lines of business often share information in common and their work processes are interconnected. As a result, the suite of systems stores redundant data and documents, and it can be difficult to share information and coordinate work processes across systems.

These inefficiencies are being addressed, in part, through emphasis on technical standards, which will establish a framework to align investments with business and technology priorities and increase interoperability among technical solutions. The Judiciary's technical standards management process provides a structured and transparent approach to develop, review, and adopt technical standards, including feedback from Judiciary stakeholders.

The Judiciary will further benefit both technically and programmatically by integrating its national systems and information. Eliminating multiple data repositories reduces data entry costs; it also eliminates the need to synchronize data across repositories, making data more consistent. The ability to share information easily and coordinate work processes across lines of business improves quality of service and increases productivity. Additionally, the ready availability of comprehensive and complete data across lines of business makes it possible to more effectively analyze organizational patterns and trends which, in turn, results in better planning and decision-making.

The Judiciary's efforts to manage data as an enterprise asset are guided by a data strategy and governance plan developed in 2015. The plan, which is overseen by the AO Data Governance Board, identifies key activities, roles and responsibilities, and measures of success. It covers caseload, defender, finance and budget, human resources, probation and pretrial services, and space and facilities data. The plan's data vision is for the Judiciary to use data effectively in a consistent, reliable, and non-biased manner to inform decisions that are made to support its mission, including but not limited to the setting of policy and the allocation of resources. With input from the AO Data Governance Board, focus on achieving this vision over the last year has been on the following priorities:

Court Unit Dashboard: The dashboard is an interactive, easy to use, graphic display of court unit data that combines multiple sources of data (including caseload, staffing, and other relevant information) into a single interface, enabling powerful insights and enhanced analysis and reporting. In addition to the Court Unit Dashboard development, the Bankruptcy Caseload Explorer, the third and final product in the Caseload Explorer suite, was launched, providing Judiciary users greater accessibility and visibility to bankruptcy caseload data.

Enterprise business glossary: This will establish a common vocabulary and help communicate and govern the definition of business terms used within the AO. Through a collaborative approach involving data stakeholders from across the AO, work on developing definitions continued and drafting of an AO policy on use of the glossary began. To date, more than 150 definitions have been agreed to, with a focus on terms found in the Court Unit Dashboard.

Data literacy: This is defined by Gartner[4] as "the ability to read, write and communicate data in context" or "speaking data." Increasing data literacy throughout the Judiciary is essential as technological advances allow for both creation and consumption of an ever-increasing amount of data. With an initial focus on the analytic tools available from the AO, the goal is to ensure that Judiciary users understand what the data represents and the source from which it comes, how it is or could be used, and who can distribute, access, and share the data.

Enterprise data management: To continue its evolution towards self-service analytics and better governed data, the AO has entered the procurement phase for the implementation of a new data governance and data management tool. This tool will help better catalog the Judiciary's data, set boundaries for the use of business glossaries and structured definitions, and continue efforts to develop data models for all current and planned data systems. A data model allows the business users to set the course for what data is included in a system and how it relates to all the other data in that system. These efforts will support increased transparency and access to data through the ability to trace data lineage and create a data catalog that clearly describes what the data is, where it is sourced from, and what can be done with it.

Judiciary Data Working Group: The group was re-chartered in 2015 and three new judge positions were

[4] Gartner is a leading research and advisory company. More information is available at https://www.gartner.com/en/about.

added to include liaisons from three Judicial Conference committees that are significant stakeholders of data, including the Committees on Information Technology, Court Administration and Case Management, and Judicial Resources.

Data strategy and governance plan update: The current plan was developed in 2015 and, while much progress has been made, a refresh is needed to the approach and priorities. While many of the plan's goals have been met, fully or partially, others have not due to shifting priorities and resources. The AO has begun the process of working with stakeholders from across the AO to update the plan to reflect the current needs and priorities to drive the Judiciary's data governance and data literacy towards greater maturity.

More Fully Utilize Local Systems

Goals of the national IT program include developing and maintaining technology standards for local IT staff to ensure compatibility with national applications as well as identifying common technology solutions to provide capabilities that reduce the proliferation of competing technology solutions. Nationally supported systems provide economies of scale, are critical to courts without the resources to develop their own systems, and provide some degree of standardization that allows courts, attorneys, and the public to share information more effectively.

Although courts share the same general business processes, the details of how they carry out those processes can vary widely. Many of these variations reflect business needs and are shaped by factors such as the type of cases that may predominate in a particular district, the size of the district, and the requirements of judicial discretion. To accommodate these variations, respond to a particular court's business needs and priorities, and address requirements not met by national systems, the Judiciary's national case management systems allow for individual court customization.

For the same reasons, courts also create adjunct systems, the requirements for which may be unique to an individual court or common to many courts. A priority of the national IT program is to facilitate sharing of local applications among courts and, where appropriate, make the functionality available nationally by incorporating those applications into national systems or by providing national support. For example, two calendaring applications[5] developed by local courts have been supported nationally for several years and are used by many judges and chambers staff. In addition, a local application called Citation Links, which was already being used by 17 courts (see Judges and Chambers Staff section), has been added to NextGen CM/ECF. This model of incorporating valuable local developments into national systems will continue to be applied in the future.

Efforts to leverage the national systems infrastructure to support locally developed administrative applications continue. Two examples are the Judiciary Inventory Control System (JICS), developed by the Northern District of New York district court, and JFinSys, a financial application developed by the Eastern District of Virginia bankruptcy court. The goal is to share the responsibility for implementing and supporting these critical functions and take advantage of the expertise that exists at the local courts and the AO. The Judiciary continues to look for similar opportunities.

To promote Judiciary-wide technical standards and enhance interoperability, a technical standards management process has been established. Technology best practices are also being identified to promote local or national applications having the greatest impact on court operations. Furthermore, a catalog of national applications has been developed and will be extended to include locally developed applications to avoid duplication of efforts, encourage collaboration, highlight gaps in the functionality of national applications, and promote communities of practice and technology knowledge-sharing. Finally, technology solutions are being developed to efficiently deploy software from the local to the national level and eventually to commercial cloud environments.

Develop system-wide approaches to the utilization of technology to achieve enhanced performance and cost savings.

The Judiciary continues to seek productivity enhancements and cost avoidance from new or improved IT systems, which provide efficiencies and help contain growth in future technology and staffing costs. Moreover, investments that reduce the complexity of IT systems also have the potential to produce savings and cost

[5] Chambers Electronic Organizer (CEO) and Chambers Automation Program (CHAP).

avoidances. The Judiciary's reliance on IT means that failure of its technical infrastructure can effectively bring operations to a halt for its internal stakeholders and severely affect the work of its external stakeholders. Therefore, reducing the complexity of the infrastructure and building a stable, reliable national infrastructure that helps avoid downtime, rework, and inefficiencies have been and remain objectives of the Judiciary's IT program. Areas on which the Judiciary will place especially high priority over the next three to five years are described below.

Network Enhancements

Increased demand on the Judiciary's communications networks both to support internal systems and to enable more widespread use of its public-facing technologies requires that network capabilities be evaluated and upgraded on an ongoing basis. The Judiciary has completed the convergence of network services, delivering voice, data, and video services over a single, secure network. The converged network offers improved delivery of other services, including mobile computing, videoconferencing in the courtroom and elsewhere, delivery of distance training through collaborative technologies, integration of telecommunications with the Judiciary's software systems, and improved ability to support server centralization. Upgrading the data center core switching infrastructure has positioned the Judiciary for data center flexibility and stability over the next decade. The completion of the Wide Area Network (WAN) Diversity project increased the overall network availability and reliability through carrier diversity and redundant connections.

A new initiative on the horizon is Software-Defined Wide Area Network (SD-WAN), which will enable administrators to match the behavior of the network environment to business priorities, routing traffic based on destination, application, and network status. With the advent of application centralization and data center consolidation as well as the move to public cloud providers, the WAN needs to become more dynamic and tuned to peak performance to maximize the use of low-cost circuits for lower priority applications. The SD-WAN will provide the Judiciary the ability to dynamically route, monitor, and measure real-time traffic to optimize performance. A plan is being developed to upgrade the data communications network (DCN) WAN router infrastructure to support this capability, including evaluation of the data center network infrastructure and development of architectural requirements needed to improve network and server performance.

Enterprise Operations Center

The Judiciary has established an Enterprise Operations Center (EOC), which will provide 24/7/365 monitoring of the national infrastructure, services, and applications to identify IT issues before they impact end users. The EOC will support all national infrastructure and applications from one operations center and serve as the single service desk and interface for any incident related to national infrastructure and applications.

Over the next few years, the EOC will consolidate several disparate national IT support functions and provide central oversight of incident and problem resolutions. The EOC will go beyond user support to monitor the national infrastructure and applications to reduce the frequency and duration of outages. New operational analyses and IT service management tools will be coupled with existing tools to increase and enhance operational visibility into all layers of the national IT infrastructure. Historical and real-time data will be used to forecast potential problems, take corrective actions, and provide clear communications to users.

Enhanced Hosting Services

The network also provides a foundation for enhancing centralized hosting services. The Judiciary continues to implement full enterprise, national-level hosting and cloud computing services in courts, including infrastructure and other hardware, database storage, computer applications, and server support. These services provide enhanced availability of Judiciary data and systems as well as an evolving catalog of cloud-

based solutions to the courts. These solutions can spur innovation, improve disaster recovery capabilities, and support a more mobile work force.

The design and implementation of a hybrid cloud will integrate the current on-premise Judiciary cloud with the best and most secure commercial offerings available. The acquisition of commercial cloud services will allow the Judiciary to self-provision computing resources to quickly meet individual business needs on a pay-as-you-go basis. The Judiciary's coordinated program will consider the potential cost, security, architectural impact, and other implications of cloud computing to provide guidance on these decisions. The overall benefit will be to increase the flexibility, efficiency, and resilience of the computing environment.

Courtroom Technologies

The Judiciary has made substantial investments in courtroom technologies that reduce trial time and litigation costs, as well as improve fact-finding, understanding by the jury, and access to court proceedings. These technologies include evidence presentation, videoconferencing, assisted listening systems, and language interpretation systems. Evidence presentation technology supplied by the court helps to level the playing field in the courtroom, preventing a mismatch of resources in which one litigant has the resources to make technologically advanced presentations and the other does not; such a mismatch could unfairly influence jurors' perceptions and the outcome of a trial.

Judiciary-wide guidelines for courtroom technologies serve as a baseline for the introduction of current and next-generation tools and capabilities. Research and proof-of-concept projects on technologies that will facilitate the efficiency of trials and hearings are ongoing and have included automated audio storage of court proceedings, networked audiovisual solutions, configured control systems (potentially replacing programmed control systems), cost reduction solutions, and training solutions. Improvements and efficiencies are being realized from digital video as well as centralization of audio, video evidence presentation, and videoconferencing systems. Rapid changes in the audiovisual industry have changed the way technologies are implemented within the courtroom and courthouse, but also present maintenance challenges, as suppliers regularly transition support to newer technologies.

EXHIBIT | D12

Communications

In 2014, the Judiciary began the process of replacing its aging enterprise messaging system with a comprehensive, unified communications solution. The widespread adoption of mobile computing, document-sharing, and collaboration, as well as the dramatic shift in the market for messaging systems, necessitated this move. After developing high-level requirements and a cost estimate, migration options were evaluated, hosting decisions made, architectural engineering completed, and an implementation plan developed. The migration to this new system, which utilizes the Microsoft Office 365 platform, is complex and touches every Judiciary user and business process that utilizes email, instant messaging, word processing, spreadsheets, and collaboration tools. The deployment of the Microsoft Office 365 ProPlus software to all Judiciary users was completed by March 2019. The migration of all Lotus Notes Mail files to Microsoft Outlook was completed by January 2020.

As Microsoft continues to add additional features to the Office 365 platform, the AO will continue to evaluate how to leverage those capabilities throughout the Judiciary. The focus will be on user adoption of Office 365, Microsoft Outlook, and OneDrive, while new tools such as Microsoft Teams, PowerAutomate, PowerApps, Stream, and Delve are introduced.

SharePoint Online (SPO) is the main collaboration and document management tool within Microsoft's Office 365 platform. SPO supports functionality to collaborate, share, and store information across the Judiciary in a way that was previously not possible. AO staff identified requirements and configured the tool, developed governance and training, and established various support processes/services to support SPO implementation across the Judiciary. The AO has been working with court unit pilots since fall of 2018 and began a waved Judiciary-wide implementation in October 2019.

Deployment waves last a calendar quarter and were scheduled to be completed by July 2020. The SPO Center of Excellence provides governance/guidance, best practices, Judiciary use cases, and training schedules. The AO is assisting individual or groups of courts through opportunities and challenges and developing videos highlighting Judiciary/court type-specific use cases, tips and tricks, and demonstrations of important features.

Refine and update security practices to ensure the confidentiality, integrity, and availability of Judiciary-related records and information.

The national IT security program protects Judiciary information systems, services, and data against disclosure, unauthorized use, modification, damage, inaccessibility, and loss. In collaboration with the court community, this program fosters a security-aware culture and promotes support for initiatives that preserve the confidentiality, integrity, and availability of information associated with all forms of technology used by the Judiciary. The program provides the Judiciary with the information needed to make informed, risk-based decisions essential to safeguarding the deliberative process.

Technology introduces security risks that need to be managed on an ongoing basis, and the Judiciary faces the challenge of balancing the benefits of these technologies with those risks. The internet, as well as the Judiciary's DCN, its underlying infrastructure, the applications that serve its mission, and the people who interact with these systems, are vulnerable to a wide range of cyber threats and hazards. In part, sophisticated attackers aim to exploit vulnerabilities to disrupt operations, gain access to sensitive court work products for financial or political gain, or simply to cause embarrassment, and are continuously developing new capabilities to interrupt, destroy, or threaten the delivery of essential services. Addressing these threats requires the use of multiple measures in the following areas: 1) preventing malicious activity; 2) detecting, analyzing, and mitigating intrusions; and 3) shaping the cybersecurity environment.

EXHIBIT | D13

Underpinning each of these is a tiered security architecture that separates resources based on data, business criticality, and function. Robust planning provides for continuous evaluation and improvement to adapt to the ever-changing threat environment and helps ensure that resources are focused where they provide the most benefit. The resulting data are analyzed to determine areas of vulnerability; to identify and respond to attack patterns and trends; and to update and continuously improve policies, procedures, and technologies commensurate with risk.

Judiciary IT security responsibilities are shared by the national program, court units, and individual users. The national program promotes secure coding practices and architectural design, maintains a 24/7 security operations capability, provides security assessment and testing services, and conducts risk-based planning, among other activities. It also encourages court units to implement analogous concepts within their environments using network segmentation techniques, security policies, privilege management, and related activities. Finally, it promotes an understanding of risk and a desire toward end-user behavior that safeguards Judiciary assets and data.

Preventing Malicious Activity

The Judiciary implements a defense-in-depth strategy designed to protect networks and information through preventative measures. Network and host-based systems are employed to routinely inspect traffic for signs of malicious activity that can be blocked or identified for further analysis. Services, tools, and devices—such as firewalls (both network and web application) at the boundaries between a court unit and the DCN

as well as between the DCN and the internet—further prevent breaches (as do network access controls, endpoint protection systems, encryption solutions, and patch management solutions). Identity and access management systems restrict access rights to Judiciary data, and web-based threat protection systems prevent end user access to known malicious sites on the internet. Finally, continuous security testing and assessments proactively identify vulnerabilities for corrective action before they can be exploited. Over the next three to five years, the AO intends to focus its efforts in this category in the following areas:

Annual IT security self-assessments: Each Judiciary unit (court unit and FPDO) assesses the effectiveness and maturity of its local IT security program using a common rubric. Results are submitted locally, at the circuit level, and to the national program for analysis and potential identification of areas for improvement in both the local and national security program. The areas assessed by this program evolve over time to incrementally improve the security baseline and to address emerging threats. The third annual Judiciary unit self-assessment period concluded in December 2019. Based on an analysis of data collected to date, including validations performed of 2018 results during the mandatory independent court unit IT security assessments, the AO has made minor refinements for the upcoming self-assessment period. Additionally, each national program office assesses the effectiveness and maturity of security programs supporting national systems, such as case management (CM/ECF and PACTS), JIFMS, and identity management. The second annual national systems self-assessment period concluded in December 2019.

Mandatory independent court unit IT security assessments: This program launched in 2018. At least once every five years, each court unit receives a comprehensive independent assessment of its management, technical, and operational safeguards to understand its strengths and weaknesses. Court units also receive feedback on the efficacy of the self-assessment program within their court unit. Assessed court units document the actions they plan to take in response to identified risks and share their action plans with the assessment team.

Secure coding practices in Judiciary applications: In 2018, the AO focused more closely on integrating secure coding practices into Judiciary software development, expanding the program with additional personnel and a more comprehensive objective. New static code analysis tools and open-source library vulnerability scanning software have allowed the AO to better prevent and detect coding vulnerabilities in judicial applications. Dedicated AO personnel regularly engage with court and national program software development teams to educate, assist in the integration of these tools in software builds, and to emphasize the importance of secure software development throughout the full lifecycle of applications. In 2020, the AO included secure coding metrics in the National System IT Security Scorecard, reinforcing the importance of this program.

Increasing the use of the web application firewalls (WAF): To better protect internet-facing Judiciary web applications from malicious activity, the AO engages with courts and national program offices to help them understand how a WAF favorably differs from a traditional firewall. WAFs provide a finer granularity of protection for web-based applications and can also be used to temporarily address some web vulnerabilities until they can be corrected in the application itself. Increasingly, courts are placing their CM/ECF applications behind the WAF to better protect them from malicious web traffic and external screen-scraping software that detrimentally affects the performance of court websites.

Judiciary Bug Bounty: Beginning in 2019, the AO has contracted a trusted firm to reward certain vetted third parties for information about any vulnerabilities or weaknesses they are able to identify in the Judiciary's public-facing infrastructure that could allow hackers to compromise Judiciary systems, applications or data. This program provides additional continual penetration testing against the Judiciary, resulting in valuable findings about real-world attack paths hackers could use. The AO validates these findings and provides detailed reports about them to courts and national program offices, complete with risk-mitigation recommendations.

Secure Socket Layer (SSL) decryption: Security devices monitor network traffic 24/7 with event logs aggregated and reviewed for evidence of malicious activity. The capability to inspect SSL traffic has been added to this process, which facilitates discovery of malicious activity that previously would have gone undetected. SSL decrypted traffic accounts for over 41 percent of all cyberattacks currently detected by the

Judiciary. The data gathered has enabled the Judiciary to proactively block attackers to prevent any disruption or degradation to essential services.

National logging service: This centrally managed service enables courts and national program offices to collect, retain, search, alert, report, and analyze large volumes of computer-generated log messages in real-time to identify and troubleshoot both general and security-related IT incidents. This service is the main tool being utilized by the EOC to move toward proactively acting on identified issues before they impact the national infrastructure.

Judiciary firewall service: The Judiciary has installed a dedicated security appliance (firewall) to the boundary between each court and the DCN, reducing the likelihood that a malicious event will spread laterally among courts. Its placement ensures a consistent configuration across locations and complements the security infrastructure at the Judiciary data centers. The Judiciary has implemented additional capabilities of these firewalls, such as vulnerability protection, spyware, and antivirus blocks, and URL filtering, which controls access to known hostile websites.

Enhanced network segmentation: This will enhance the security of network resources by restricting access to specific network segments based on user access authorization and on the health and/or location of the device attempting to connect to them, and only allowing access to the minimum network resources required to perform a given function or task. This initiative will be conducted in an incremental, phased approach with the initial focus being on segmentation of DCN resources.

Security infrastructure modernization for remote access: The Judiciary is assessing existing remote access services, products, and infrastructure for opportunities to enhance the remote access program, particularly for providing DCN access to a variety of devices. The Judiciary also is considering moving toward a Zero Trust Architecture, an information security model that requires verification for every user and device attempting to access an organization's network resources, regardless of how a device was furnished (e.g., by the Judiciary, personally owned, or other devices such as a hotel kiosk) and limits network resources to only those needed by the user.

Detecting, Analyzing, and Mitigating Intrusions

Activities in this area allow the Judiciary to react quickly and effectively to suspected security incidents. These activities include analyzing indicators of malicious activity detected by the mechanisms previously described, including event notification, remediation support, and data forensics. They also include event correlation and analysis of activities across multiple services, tools, and devices. These activities address the impact of intrusions on systems and applications, including incident response plans, log analysis and review, and actions to redress exploited vulnerabilities. Keeping these capabilities current requires continually evaluating cyber threat trends and their potential impact on Judiciary assets as well as incorporating data derived from new tools. Priority efforts in this area will include the following:

Log management, analysis, and notification: National logging and firewall services deployed throughout the Judiciary generate a wealth of new information which the AO must analyze for threat indicators so that alerts are triggered and court notifications are sent in a timely manner. While additional data sources have been added from cloud environments and local court endpoints, existing technology suites still require improvements to their configuration and management to make their output suitable for analysis with machine learning and other advanced techniques.

Data management: The Judiciary continues to seek ways to more effectively collect data, analyze it, and translate it into actionable information. For example, within the national IT security program, the AO applies data visualization and risk management tools to the annual court unit IT security self-assessment data and national system security self-assessment data to understand the impact of national IT security investments on enterprise security. These methods also help the AO to identify areas in which the self-assessment process supporting documentation needs improvement.

Forensics: Digital forensic analysis is pivotal in determining the timeline and root causes of critical security incidents. Investments since last fiscal year have significantly improved the ability of security analysts to triage potential intrusions in order to prioritize investigations and identify the vulnerabilities exploited by hackers that require immediate remediation.

Red Team service: Using tactics commonly employed by the hacker community, Red Team services validate network defenses by identifying vulnerabilities to inform and enable continuous improvement. The existing Red

Team personnel currently alternate between discrete iterations of a continuous exercise against the AO's infrastructure and fulfilling court requests for stand-alone adversary-emulation exercises. Planned expansion of the program will increase both the number of courts that can benefit from this service, and the frequency of iterations in the exercise against the AO.

Hunt Team service: In order to identify any potential cyber-adversaries deeply embedded within the Judiciary network, a specialized team of security professionals proactively and systematically searches for evidence of known cyber-criminal tools, tactics, and techniques. This team also investigates abnormal user and machine behavior. Hunt operations are pivotal in adding context to, and expanding, the scope of investigations across the enterprise.

Shaping the Cybersecurity Environment

The Judiciary creates and maintains a security-aware culture using recognized best practices for information security. Development and oversight of the Judiciary Information Security Framework (Framework) provides the foundation to effectively manage risks, make informed decisions about implementing safeguards, and continually assess safeguards for suitability and effectiveness. Policies, tools, and other resources facilitate implementation of Framework concepts across the Judiciary. As IT security is a shared responsibility, court units and FPDOs need policies, tools, information, and education to perform their role. Over the next three to five years, the AO intends to focus its efforts in this category in the following areas:

Vulnerability prioritization: The AO plans to improve the Judiciary's ability to identify and prioritize remediating the vulnerabilities that pose the highest risk to Judiciary systems and networks. This process involves correlating vulnerability threat information with data from existent scanning tools, alerting courts and national programs about the increased risk of these particular vulnerabilities, and, when necessary, initiating additional out-of-cycle remediation processes.

EXHIBIT | D16

IT security education: The IT security training curriculum continues to expand and evolve to meet the ever-changing IT security needs of the Judiciary. The program, launched in 2017, continues to evolve and includes course offerings which provide court and FPDO IT security professionals with the knowledge required to pursue nationally recognized cybersecurity certifications while at the same time delivering in-depth training on the security tools utilized by the Judiciary. Training offerings continue to raise the level of cybersecurity knowledge and skills in the Judiciary. As the cybersecurity landscape changes, new training curriculums will be offered enabling IT security professionals to acquire the skills necessary for the Judiciary to stay abreast of IT security needs.

New security tools: Data from the Judiciary's cybersecurity efforts is continually analyzed to assess the need to modify or add tools to address vulnerabilities. As part of this effort, security solutions in the area of privileged account management are currently being deployed. A migration to a new endpoint protection tool is being planned for late calendar year 2020 to 2021. In addition, best practices are being developed regarding deployment of application "whitelisting" and file integrity monitoring tools. Licensing, hosting, training, and implementation strategies are being developed to effectively deploy these security tools.

Cyber threat intelligence: Open-source intelligence collection and analysis strengthens the national IT security program by identifying new vulnerabilities, detecting imminent threats, identifying attack trends using metrics, and coordinating with external partners in law enforcement, other government agencies, and non-government organizations to act on credible indicators of harm. Intelligence analysts enhance situational awareness and provide threat attribution to bring context to threats targeting the Judiciary. Efforts are underway to gain access to additional facilities and systems to better monitor for threats targeting the Judiciary.

Investing in the IT Program

The Judiciary aligns its IT investments with its business objectives through an inclusive planning process that is synchronized with the Judiciary's budget cycle. The Judicial Conference Committee on Information Technology reviews resource requirements and expenditure plans for the Judiciary's IT program in accordance with guidelines and priorities established by the Judicial Conference for the use of available resources.

When considering the costs associated with the IT program, it is important to take a broad Judiciary-wide view. The Judiciary's public-facing technologies, internal systems, technical infrastructure, and security program have resulted in improved services to its external stakeholders as well as internal efficiencies that have allowed the courts to absorb an increased workload without increasing staff as much as would otherwise have been required. These cost avoidances will become increasingly important in times of continuing budgetary constraints.

The Judiciary will continue to rely heavily on its IT program to meet its mission and to serve the public in the coming years. As indicated in this annual update to the Long Range Plan, not only will existing systems and infrastructure be maintained and enhanced, but emphasis will be placed on adopting new systems, technologies, and services that will provide additional benefits.

The table below shows the Judiciary's anticipated IT resource requests for fiscal years 2021 through 2025, organized by category within the Judiciary Information Technology Fund (JITF).[6] Successful execution of the objectives in this plan is dependent on the availability of funding. Each category is described in the next section.

Resource Requirements

	Current Estimate (Dollars in Millions)				
JITF Program Component	**FY 2021**	**FY 2022**	**FY 2023**	**FY 2024**	**FY 2025**
Administrative and Management Systems	$75.7	$75.7	$107.5	$103.9	$105.4
Court Administration and Case Management	28.2	29.2	42.0	46.0	41.5
Court Allotments	106.3	104.0	107.4	109.0	109.7
Court Support	71.5	74.8	77.5	79.1	80.6
Infrastructure and Collaboration	135.7	135.8	160.0	164.0	180.7
Judicial Statistics and Reporting	17.1	17.2	24.2	24.4	24.7
Telecommunications	95.9	102.8	117.3	115.3	111.7
Subtotal	$530.4	$539.5	$635.9	$641.7	$654.3
Electronic Public Access Program	159.5	163.4	187.0	191.4	184.8
Total JITF Financial Requirements	$689.9	$702.9	$822.9	$833.1	$839.1

[6] Section 612 of Title 28, United States Code, establishes the JITF and makes funds available to the Judiciary's information technology program without fiscal year limitation.

JITF Program Components

Administrative and Management Systems

This program includes the Judiciary's financial and personnel management systems, as well as systems to support and manage space and facilities projects and travel expenses and Judiciary websites.

Court Administration and Case Management

This category contains a variety of tools, including the probation and pretrial services case management system; tools to access critical case information and law enforcement databases; systems for juror qualification, management, and payment; tools for jury participants to communicate with the courts; as well as the system that captures requests for payments to private court-appointed counsel and expert service providers.

Court Allotments

These funds are allotted to the courts to pay directly for operating, maintaining, and replacing computers, printers, LAN equipment, and software as well as local telecommunications services, equipment, maintenance, and courtroom technology.

Court Support

Court support funds AO staff that provide IT development, management, and maintenance services to the courts. These services include IT policy and planning guidance; architecture and infrastructure support; security services; development, testing, and implementation of national IT applications; IT training; and other administrative and IT support services on behalf of the courts.

Infrastructure and Collaboration Tools

This category encompasses building and maintaining a robust, reliable, and resilient Judiciary-wide IT infrastructure. Included are the costs of hardware, software, and IT security associated with the Judiciary's full enterprise hosting and cloud computing services and email and collaboration systems. It also includes the costs of IT infrastructure for new courthouse construction projects and operating systems support, maintenance, testing, security, and research.

Judicial Statistics and Reporting

This category includes systems to support gathering and reporting statistics in the Judiciary; data analysis and management reporting across Judiciary-wide data sources, and planning and decision-making with staffing, financial, and workload data.

Telecommunications

This category includes support for voice and data transmission services and telecommunications. The Judiciary's communications program enables the Judiciary to operate communications services for the appellate, district, and bankruptcy courts as well as probation and pretrial services offices. It also enables the Judiciary to procure communications equipment for new courthouses and for courthouses undergoing major repairs and alterations.

Electronic Public Access Program

This category provides electronic public access to court information; develops and maintains electronic public access systems such as CM/ECF in the Judiciary; and provides centralized billing, registration, and technical support services for the Judiciary and the public through the PACER Service Center.

Administrative Office of the U.S. Courts

One Columbus Circle, N.E.
Washington, D.C. 20544

www.uscourts.gov

EXHIBIT | D19

ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS

One Columbus Circle NE., Washington, DC 20544
Phone, 202–502–2600

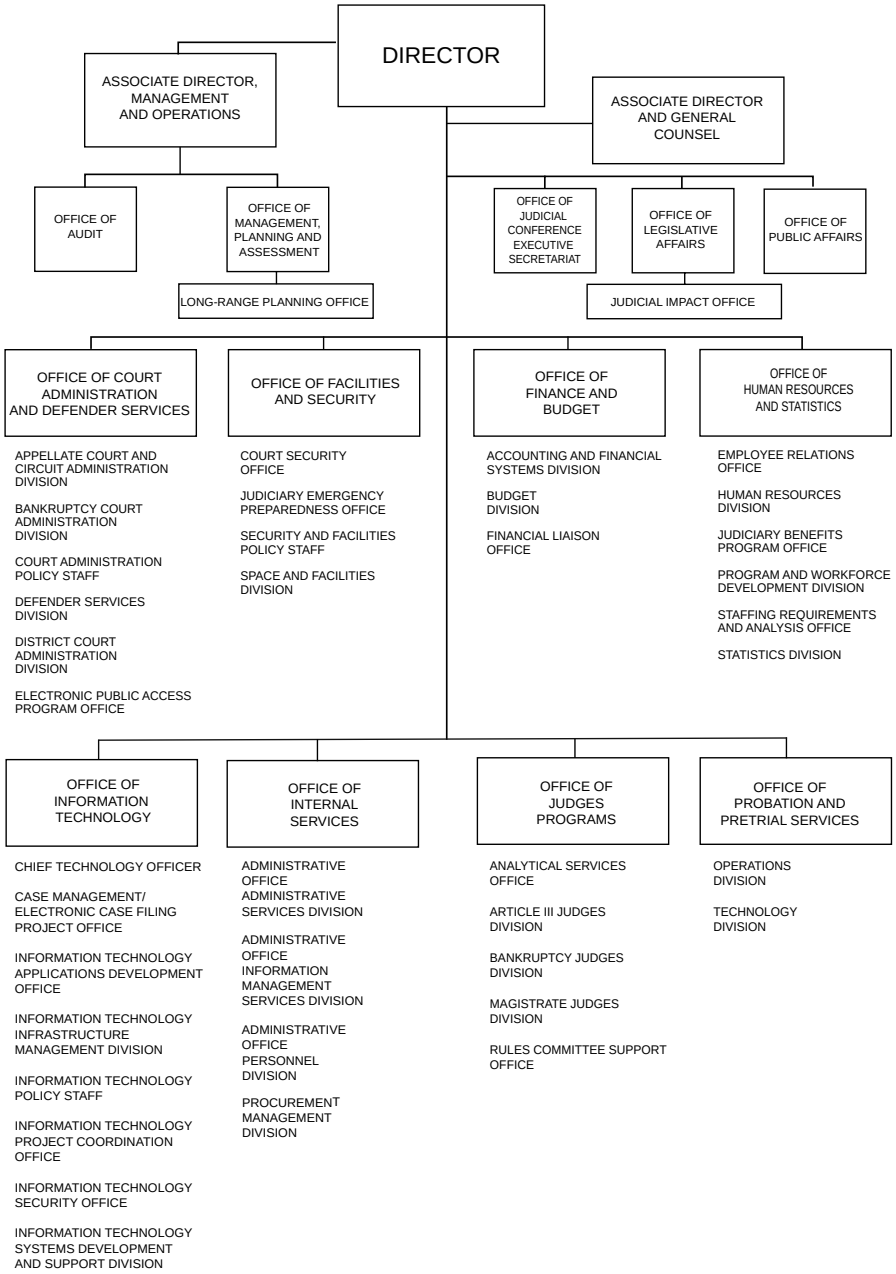
Director	LEONIDAS RALPH MECHAM
Deputy Director	(VACANCY)
Associate Director, Management and Operations	CLARENCE A. (PETE) LEE, JR.
Deputy Associate Director	CATHY A. MCCARTHY
Audit Officer	JEFFERY J. LARIONI
Management, Planning and Assesment Officer	CATHY A. MCCARTHY
Associate Director and General Counsel	WILLIAM R. BURCHILL, JR.
Deputy General Counsel	ROBERT K. LOESCHE
Assistant Director, Office of Judicial Conference Executive Secretariat	KAREN K. SIEGEL
Deputy Assistant Director	WENDY JENNIS
Assistant Director, Office of Legislative Affairs	MICHAEL W. BLOMMER
Deputy Assistant Director	DANIEL A. CUNNINGHAM
Assistant Director, Office of Public Affairs	DAVID A. SELLERS
Public Information Officer	KAREN E. REDMOND
Assistant Director, Office of Court Administration and Defender Services	NOEL J. AUGUSTYN
Deputy Assistant Director for Court Administration	GLEN K. PALMAN
Chief, Appellate Court and Circuit Administration Division	JOHN P. HEHMAN
Chief, Bankruptcy Court Administration Division	GLEN K. PALMAN
Chief, Court Administration Policy Staff	ABEL J. MATTOS
Chief, Defender Services Division	THEODORE J. LIDZ
Chief, District Court Administration Division	ROBERT LOWNEY
Chief, Electronic Public Access Program Office	MARY M. STICKNEY
Assistant Director, Office of Facilities and Security	ROSS EISENMAN
Deputy Assistant Director	WILLIAM J. LEHMAN
Chief, Court Security Office	DENNIS P. CHAPAS
Chief, Judiciary Emergency Preparedness Office	WILLIAM J. LEHMAN
Chief, Security and Facilities Policy Staff	SUSAN J. HAYES
Chief, Space and Facilities Division	RODGERS A. STEWART
Assistant Director, Office of Finance and Budget	GEORGE H. SCHAFER
Deputy Assistant Director	GREGORY D. CUMMINGS
Chief, Accounting and Financial Systems Division	PHILIP L. MCKINNEY
Chief, Budget Division	BRUCE E. JOHNSON
Financial Liaison Officer	PENNY JACOBS FLEMING
Assistant Director, Office of Human Resources and Statistics	R. TOWNSEND ROBINSON, *Acting*
Deputy Assistant Director	R. TOWNSEND ROBINSON
Chief, Employee Relations Office	TRUDI M. MORRISON

Chief, Human Resources Division	CHARLOTTE G. PEDDICORD
Chief, Judiciary Benefits Program Office	LEE HORVATH
Chief, Program and Workforce Development Division	MAURICE E. WHITE
Chief, Staffing Requirements and Analysis Office	BEVERLY J. BONE
Chief, Statistics Division	STEVEN R. SCHLESINGER
Assistant Director, Office of Information Technology	MELVIN J. BRYSON
Deputy Assistant Director	BARBARA C. MACKEN
Chief Technology Officer	RICHARD D. FENNELL
Chief, Case Management/Electronic Case Files Project Office	GARY L. BOCKWEG
Chief, Information Technology Applications Development Office	WENDY LAGEMAN
Chief, Information Technology Infrastructure Management Division	CRAIG W. JENKINS
Chief, Information Technology Policy Staff	TERRY A. CAIN
Chief, Information Technology Project Coordination Office	FRANK D. DOZIER, *Acting*
Chief, Information Technology Security Office	ROBERT N. SINSHEIMER
Chief, Information Technology Systems Deployment and Support Division	HOWARD J. GRANDIER
Assistant Director, Office of Internal Services	LAURA C. MINOR
Deputy Assistant Director	NANCY LEE BRADSHAW
Chief, Administrative Services Division	DOREEN G.B. BYDUME
Chief, Information Management Services Division	JOHN C. CHANG
Chief, Administrative Office Personnel Division	CHERI THOMPSON REID
Chief, Procurement Management Division	ARNOLD J. GILDENHORN
Assistant Director, Office of Judges Programs	PETER G. MCCABE
Deputy Assistant Director for Policy Development	JEFFREY A. HENNEMUTH
Chief, Analytical Services Office	ELLYN L. VAIL
Chief, Article III Judges Division	MARGARET A. IRVING, *Acting*
Chief, Bankruptcy Judges Division	FRANCIS F. SZCZEBAK
Chief, Magistrate Judges Division	THOMAS C. HNATOWSKI
Chief, Rules Committee Support Office	JOHN K. RABIEJ
Assistant Director, Office of Probation and Pretrial Services	JOHN M. HUGHES
Deputy Assistant Director	MATTHEW ROWLAND
Head, Operations Division	CAROLYN YN CABELL
Head, Technology Division	NICHOLAS B. DISABATINO

The Administrative Office of the United States Courts is charged with the nonjudicial, administrative business of the United States Courts, including the maintenance of workload statistics and the disbursement of funds appropriated for the maintenance of the U.S. judicial system.

The Administrative Office of the United States Courts was created by act of August 7, 1939 (28 U.S.C. 601). The Office was established November 6, 1939. Its Director and Deputy Director are appointed by the Chief Justice of the United States after consultation with the Judicial Conference.

ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS



Administering the Courts The Director is the administrative officer of the courts of the United States (except the Supreme Court). Under the guidance of the Judicial Conference of the United States the Director is required, among other things, to

—supervise all administrative matters relating to the offices of clerks and other clerical and administrative personnel of the courts;

—examine the state of the dockets of the courts, secure information as to the courts' need of assistance, and prepare and transmit quarterly to the chief judges of the circuits statistical data and reports as to the business of the courts;

—submit to the annual meeting of the Judicial Conference of the United States, at least 2 weeks prior thereto, a report of the activities of the Administrative Office and the state of the business of the courts;

—fix the compensation of employees of the courts whose compensation is not otherwise fixed by law;

—regulate and pay annuities to widows and surviving dependent children of judges;

—disburse moneys appropriated for the maintenance and operation of the courts;

—examine accounts of court officers;

—regulate travel of judicial personnel;

—provide accommodations and supplies for the courts and their clerical and administrative personnel;

—establish and maintain programs for the certification and utilization of court interpreters and the provision of special interpretation services in the courts; and

—perform such other duties as may be assigned by the Supreme Court or the Judicial Conference of the United States.

The Director is also responsible for the preparation and submission of the budget of the courts, which shall be transmitted by the Office of Management and Budget to Congress without change.

Probation Officers The Administrative Office exercises general supervision of the accounts and practices of the Federal probation offices, subject to primary control by the respective district courts that they serve. The Office publishes quarterly, in cooperation with the Bureau of Prisons of the Department of Justice, a magazine entitled *Federal Probation,* which is a journal ''of correctional philosophy and practice.''

The Director also has responsibility with respect to the establishment of pretrial services in the district courts under the Pretrial Services Act of 1982 (18 U.S.C. 3152). These offices report to their respective courts information concerning pretrial release of persons charged with Federal offenses and supervise such persons who are released to their custody.

Bankruptcy The Bankruptcy Amendments and Federal Judgeship Act of 1984 (28 U.S.C. 151) provided that the bankruptcy judges for each judicial district shall constitute a unit of the district court to be known as the bankruptcy court. Bankruptcy judges are appointed by the courts of appeals in such numbers as authorized by Congress and serve for a term of 14 years as judicial officers of the district courts.

This act placed jurisdiction in the district courts over all cases under title 11, United States Code, and all proceedings arising in or related to cases under that title (28 U.S.C. 1334). The district court may provide for such cases and proceedings to be referred to its bankruptcy judges (as authorized by 28 U.S.C. 157).

The Director of the Administrative Office recommends to the Judicial Conference the official duty stations and places of holding court of bankruptcy judges, surveys the need for additional bankruptcy judgeships to be recommended to Congress, and determines the staff needs of bankruptcy judges and the clerks of the bankruptcy courts.

Federal Magistrate Judges The Director of the Administrative Office exercises general supervision over administrative matters in offices of U.S. magistrate judges, compiles and evaluates statistical data relating to such offices, and submits reports thereon to the Judicial Conference. The Director reports annually to Congress on the business that has come before U.S. magistrate judges and also prepares legal and administrative manuals for the use of the

magistrate judges. The act provides for surveys to be conducted by the Administrative Office of the conditions in the judicial districts in order to make recommendations as to the number, location, and salaries of magistrate judges, which are determined by the Judicial Conference subject to the availability of appropriated funds.

Federal Defenders The Criminal Justice Act (18 U.S.C. 3006A) establishes the procedure for the appointment of private panel attorneys in Federal criminal cases for individuals who are unable to afford adequate representation, under plans adopted by each district court. The act also permits the establishment of Federal public defender or Federal community defender organizations by the district courts in districts where at least 200 persons annually require the appointment of counsel. Two adjacent districts may be combined to reach this total.

Each defender organization submits to the Director of the Administrative Office an annual report of its activities along with a proposed budget or, in the case of community defender organizations, a proposed grant for the coming year. The Director is responsible for the submission of the proposed budgets and grants to the Judicial Conference for approval. The Director also makes payments to the defender organizations out of appropriations in accordance with the approved budgets and grants, as well as compensating private counsel appointed to defend criminal cases in the United States courts.

Sources of Information

Information may be obtained from the following sources:

Bankruptcy Judges Division. Phone, 202–502–1900.

Budget Division. Phone, 202–502–2100.

Defender Services Division. Phone, 202–502–3030.

General Counsel. Phone, 202–502–1100.

Human Resources Division. Phone, 202–502–3100.

Judicial Conference Executive Secretariat. Phone, 202–502–2400.

Legislative Affairs Office. Phone, 202–502–1700.

Magistrate Judges Division. Phone, 202–502–1830.

Office of Probation and Pretrial Services. Phone, 202–502–1610.

Public Affairs Office. Phone, 202–502–2600.

Statistics Division. Phone, 202–502–1440.

For further information, contact one of the offices listed above, Administrative Office of the United States Courts, Thurgood Marshall Federal Judiciary Building, One Columbus Circle NE., Washington, DC 20544. Internet, www.uscourts.gov.

FEDERAL JUDICIAL CENTER

Thurgood Marshall Federal Judiciary Building,
One Columbus Circle NE., Washington, DC 20002–8003
Phone, 202–502–4000. Internet, www.fjc.gov.

Director	FERN M. SMITH
Deputy Director	RUSSELL R. WHEELER
Director of Research	JAMES B. EAGLIN
Director of Judicial Education	JOHN S. COOKE
Director of Court Education	EMILY Z. HUEBNER
Director of Communications Policy and Design	SYLVAN A. SOBEL

The Federal Judicial Center is the judicial branch's agency for policy research and continuing education.

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

Note to Readers on the Update

Version 1.1 of this Cybersecurity Framework refines, clarifies, and enhances Version 1.0, which was issued in February 2014. It incorporates comments received on the two drafts of Version 1.1.

Version 1.1 is intended to be implemented by first-time and current Framework users. Current users should be able to implement Version 1.1 with minimal or no disruption; compatibility with Version 1.0 has been an explicit objective.

The following table summarizes the changes made between Version 1.0 and Version 1.1.

Table NTR-1 - Summary of changes between Framework Version 1.0 and Version 1.1.

Update	Description of Update
Clarified that terms like "compliance" can be confusing and mean something very different to various Framework stakeholders	Added clarity that the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. However, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing.
A new section on self-assessment	Added Section 4.0 *Self-Assessing Cybersecurity Risk with the Framework* to explain how the Framework can be used by organizations to understand and assess their cybersecurity risk, including the use of measurements.
Greatly expanded explanation of using Framework for Cyber Supply Chain Risk Management purposes	An expanded Section 3.3 *Communicating Cybersecurity Requirements with Stakeholders* helps users better understand Cyber Supply Chain Risk Management (SCRM), while a new Section 3.4 Buying Decisions highlights use of the Framework in understanding risk associated with commercial off-the-shelf products and services. Additional Cyber SCRM criteria were added to the Implementation Tiers. Finally, a Supply Chain Risk Management Category, including multiple Subcategories, has been added to the Framework Core.
Refinements to better account for authentication, authorization, and identity proofing	The language of the Access Control Category has been refined to better account for authentication, authorization, and identity proofing. This included adding one Subcategory each for Authentication and Identity Proofing. Also, the Category has been renamed to Identity Management and Access Control (PR.AC) to better represent the scope of the Category and corresponding Subcategories.
Better explanation of the relationship between Implementation Tiers and Profiles	Added language to Section 3.2 *Establishing or Improving a Cybersecurity Program* on using Framework Tiers in Framework implementation. Added language to Framework Tiers to reflect integration of Framework considerations within organizational risk management programs. The Framework Tier concepts were also refined. Updated Figure 2.0 to include actions from the Framework Tiers.

Consideration of Coordinated Vulnerability Disclosure	A Subcategory related to the vulnerability disclosure lifecycle was added.

As with Version 1.0, Version 1.1 users are encouraged to customize the Framework to maximize individual organizational value.

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Acknowledgements

This publication is the result of an ongoing collaborative effort involving industry, academia, and government. The National Institute of Standards and Technology (NIST) launched the project by convening private- and public-sector organizations and individuals in 2013. Published in 2014 and revised during 2017 and 2018, this *Framework for Improving Critical Infrastructure Cybersecurity* has relied upon eight public workshops, multiple Requests for Comment or Information, and thousands of direct interactions with stakeholders from across all sectors of the United States along with many sectors from around the world.

The impetus to change Version 1.0 and the changes that appear in this Version 1.1 were based on:

- Feedback and frequently asked questions to NIST since release of Framework Version 1.0;
- 105 responses to the December 2015 request for information (RFI), *Views on the Framework for Improving Critical Infrastructure Cybersecurity*;
- Over 85 comments on a December 5, 2017 proposed second draft of Version 1.1;
- Over 120 comments on a January 10, 2017, proposed first draft Version 1.1; and
- Input from over 1,200 attendees at the 2016 and 2017 Framework workshops.

In addition, NIST previously released Version 1.0 of the Cybersecurity Framework with a companion document, *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*. This Roadmap highlighted key "areas of improvement" for further development, alignment, and collaboration. Through private and public-sector efforts, some areas of improvement have advanced enough to be included in this Framework Version 1.1.

NIST acknowledges and thanks all of those who have contributed to this Framework.

Executive Summary

The United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain customers. Cybersecurity can be an important and amplifying component of an organization's overall risk management.

To better address these risks, the Cybersecurity Enhancement Act of 2014[1] (CEA) updated the role of the National Institute of Standards and Technology (NIST) to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. Through CEA, NIST must identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks." This formalized NIST's previous work developing Framework Version 1.0 under Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity" (February 2013), and provided guidance for future Framework evolution. The Framework that was developed under EO 13636, and continues to evolve according to CEA, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business and organizational needs without placing additional regulatory requirements on businesses.

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles. Through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

While this document was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in any sector or community. The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience.

The Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today. Moreover, because it references globally recognized standards for cybersecurity, the

[1] *See* 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) became public law 113-274 on December 18, 2014 and may be found at: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

Framework can serve as a model for international cooperation on strengthening cybersecurity in critical infrastructure as well as other sectors and communities.

The Framework offers a flexible way to address cybersecurity, including cybersecurity's effect on physical, cyber, and people dimensions. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT). The Framework can assist organizations in addressing cybersecurity as it affects the privacy of customers, employees, and other parties. Additionally, the Framework's outcomes serve as targets for workforce development and evolution activities.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization. For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework's five Functions to analyze its entire risk management portfolio; that analysis may or may not rely on more detailed companion guidance, such as controls catalogs. There sometimes is discussion about "compliance" with the Framework, and the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. Nevertheless, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing and mean something very different to various stakeholders.

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. NIST will continue coordinating with the private sector and government agencies at all levels. As the Framework is put into greater practice, additional lessons learned will be integrated into future versions. This will ensure the Framework is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

Expanded and more effective use and sharing of best practices of this voluntary Framework are the next steps to improve the cybersecurity of our Nation's critical infrastructure – providing evolving guidance for individual organizations while increasing the cybersecurity posture of the Nation's critical infrastructure and the broader economy and society.

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Table of Contents

List of Figures

List of Tables

1.0 Framework Introduction

The United States depends on the reliable functioning of its critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain customers. Cybersecurity can be an important and amplifying component of an organization's overall risk management.

To strengthen the resilience of this infrastructure, the Cybersecurity Enhancement Act of 2014[2] (CEA) updated the role of the National Institute of Standards and Technology (NIST) to "facilitate and support the development of" cybersecurity risk frameworks. Through CEA, NIST must identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks." This formalized NIST's previous work developing Framework Version 1.0 under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," issued in February 2013[3], and provided guidance for future Framework evolution.

Critical infrastructure[4] is defined in the U.S. Patriot Act of 2001[5] as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Due to the increasing pressures from external and internal threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk. This approach is necessary regardless of an organization's size, threat exposure, or cybersecurity sophistication today.

The critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nation's infrastructure. Members of each critical infrastructure sector perform functions that are supported by the broad category of technology, including information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT). This reliance on technology, communication, and interconnectivity has changed and expanded the potential vulnerabilities and increased potential risk to operations. For example, as technology and the data it produces and processes are increasingly used to deliver critical services and support business/mission decisions, the potential impacts of a cybersecurity incident on an

[2] *See* 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) became public law 113-274 on December 18, 2014 and may be found at: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

[3] Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf

[4] The Department of Homeland Security (DHS) Critical Infrastructure program provides a listing of the sectors and their associated critical functions and value chains. http://www.dhs.gov/critical-infrastructure-sectors

[5] See 42 U.S.C. § 5195c(e)). The U.S. Patriot Act of 2001 (H.R.3162) became public law 107-56 on October 26, 2001 and may be found at: https://www.congress.gov/bill/107th-congress/house-bill/3162

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

organization, the health and safety of individuals, the environment, communities, and the broader economy and society should be considered.

To manage cybersecurity risks, a clear understanding of the organization's business drivers and security considerations specific to its use of technology is required. Because each organization's risks, priorities, and systems are unique, the tools and methods used to achieve the outcomes described by the Framework will vary.

Recognizing the role that the protection of privacy and civil liberties plays in creating greater public trust, the Framework includes a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. Many organizations already have processes for addressing privacy and civil liberties. The methodology is designed to complement such processes and provide guidance to facilitate privacy risk management consistent with an organization's approach to cybersecurity risk management. Integrating privacy and cybersecurity can benefit organizations by increasing customer confidence, enabling more standardized sharing of information, and simplifying operations across legal regimes.

The Framework remains effective and supports technical innovation because it is technology neutral, while also referencing a variety of existing standards, guidelines, and practices that evolve with technology. By relying on those global standards, guidelines, and practices developed, managed, and updated by industry, the tools and methods available to achieve the Framework outcomes will scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements. The use of existing and emerging standards will enable economies of scale and drive the development of effective products, services, and practices that meet identified market needs. Market competition also promotes faster diffusion of these technologies and practices and realization of many benefits by the stakeholders in these sectors.

Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:

1) Describe their current cybersecurity posture;
2) Describe their target state for cybersecurity;
3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4) Assess progress toward the target state;
5) Communicate among internal and external stakeholders about cybersecurity risk.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization. For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework's five Functions to analyze its entire risk management portfolio; that analysis may or may not rely on more detailed companion guidance, such as controls catalogs. There sometimes is discussion about "compliance" with the Framework, and the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. Nevertheless, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing and mean something very different to various stakeholders.

The Framework complements, and does not replace, an organization's risk management process and cybersecurity program. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

While the Framework has been developed to improve cybersecurity risk management as it relates to critical infrastructure, it can be used by organizations in any sector of the economy or society. It is intended to be useful to companies, government agencies, and not-for-profit organizations regardless of their focus or size. The common taxonomy of standards, guidelines, and practices that it provides also is not country-specific. Organizations outside the United States may also use the Framework to strengthen their own cybersecurity efforts, and the Framework can contribute to developing a common language for international cooperation on critical infrastructure cybersecurity.

1.1 Overview of the Framework

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business/mission drivers and cybersecurity activities. These components are explained below.

- The *Framework Core* is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories – which are discrete outcomes – for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.
- *Framework Implementation Tiers* ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the

characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

- A *Framework Profile* ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important; it can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

1.2 Risk Management and the Cybersecurity Framework

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts. With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance.

With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services. The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. Thus, the Framework gives organizations the ability to dynamically select and direct improvement in cybersecurity risk management for the IT and ICS environments.

The Framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes. Examples of cybersecurity risk management processes include International Organization for Standardization (ISO)

31000:2009[6], ISO/International Electrotechnical Commission (IEC) 27005:2011[7], NIST Special Publication (SP) 800-39[8], and the *Electricity Subsector Cybersecurity Risk Management Process* (RMP) guideline[9].

1.3 Document Overview

The remainder of this document contains the following sections and appendices:

- Section 2 describes the Framework components: the Framework Core, the Tiers, and the Profiles.
- Section 3 presents examples of how the Framework can be used.
- Section 4 describes how to use the Framework for self-assessing and demonstrating cybersecurity through measurements.
- Appendix A presents the Framework Core in a tabular format: the Functions, Categories, Subcategories, and Informative References.
- Appendix B contains a glossary of selected terms.
- Appendix C lists acronyms used in this document.

[6] International Organization for Standardization, *Risk management – Principles and guidelines*, ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

[7] International Organization for Standardization/International Electrotechnical Commission, *Information technology – Security techniques – Information security risk management*, ISO/IEC 27005:2011, 2011. https://www.iso.org/standard/56742.html

[8] Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, March 2011. https://doi.org/10.6028/NIST.SP.800-39

[9] U.S. Department of Energy, *Electricity Subsector Cybersecurity Risk Management Process*, DOE/OE-0003, May 2012. https://energy.gov/sites/prod/files/Cybersecurity Risk Management Process Guideline - Final - May 2012.pdf

2.0 Framework Basics

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization. Different types of entities – including sector coordinating structures, associations, and organizations – can use the Framework for different purposes, including the creation of common Profiles.

2.1 Framework Core

The *Framework Core* provides a set of activities to achieve specific cybersecurity *outcomes*, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References, depicted in **Figure 1**:

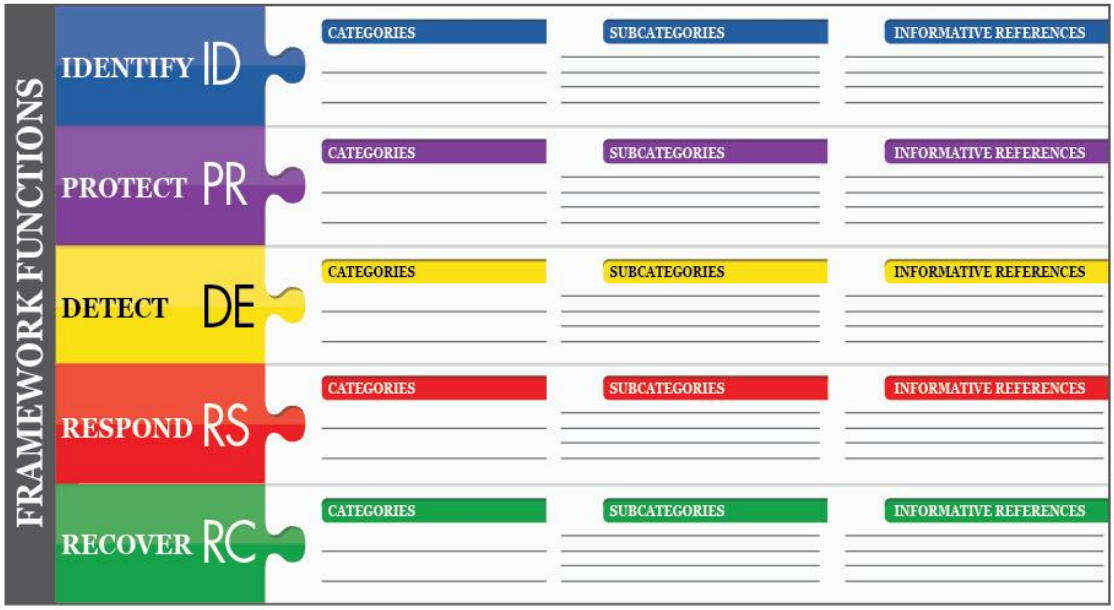


Figure 1: Framework Core Structure

The Framework Core elements work together as follows:

- **Functions** organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

- **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Identity Management and Access Control," and "Detection Processes."
- **Subcategories** further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."
- **Informative References** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process.

The five Framework Core Functions are defined below. These Functions are not intended to form a serial path or lead to a static desired end state. Rather, the Functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk. See Appendix A for the complete Framework Core listing.

- **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

  The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

- **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.

  The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

- **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

  The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

- **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

  The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

  The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

2.2 Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Ranging from Partial (Tier 1) to Adaptive (Tier 4), Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices. They help determine the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices. Risk management considerations include many aspects of cybersecurity, including the degree to which privacy and civil liberties considerations are integrated into an organization's management of cybersecurity risk and potential risk responses.

The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business/mission objectives, supply chain cybersecurity requirements, and organizational constraints. Organizations should determine the desired Tier, ensuring that the selected level meets the organizational goals, is feasible to implement, and reduces cybersecurity risk to critical assets and resources to levels acceptable to the organization. Organizations should consider leveraging external guidance obtained from Federal government departments and agencies, Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), existing maturity models, or other sources to assist in determining their desired tier.

While organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or greater, Tiers do not represent maturity levels. Tiers are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and could receive additional resources. Progression to higher Tiers is encouraged when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk.

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Successful implementation of the Framework is based upon achieving the outcomes described in the organization's Target Profile(s) and not upon Tier determination. Still, Tier selection and designation naturally affect Framework Profiles. The Tier recommendation by Business/Process Level managers, as approved by the Senior Executive Level, will help set the overall tone for how cybersecurity risk will be managed within the organization, and should influence prioritization within a Target Profile and assessments of progress in addressing gaps.

The Tier definitions are as follows:

Tier 1: Partial

- *Risk Management Process* – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- *Integrated Risk Management Program* – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
- *External Participation* – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.

Tier 2: Risk Informed

- *Risk Management Process* – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- *Integrated Risk Management Program* – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.
- *External Participation* – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks.

Tier 3: Repeatable

- *Risk Management Process* – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- *Integrated Risk Management Program* – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.
- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.

Tier 4: Adaptive

- *Risk Management Process* – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats.
- *Integrated Risk Management Program* – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.

- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it communicates proactively, using formal (e.g. agreements) and informal mechanisms to develop and maintain strong supply chain relationships.

2.3 Framework Profile

The Framework Profile ("Profile") is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs.

Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. Profiles support business/mission requirements and aid in communicating risk within and between organizations. This Framework does not prescribe Profile templates, allowing for flexibility in implementation.

Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives. An action plan to address these gaps to fulfill a given Category or Subcategory can contribute to the roadmap described above. Prioritizing the mitigation of gaps is driven by the organization's business needs and risk management processes. This risk-based approach enables an organization to gauge the resources needed (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner. Furthermore, the Framework is a risk-based approach where the applicability and fulfillment of a given Subcategory is subject to the Profile's scope.

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

2.4 Coordination of Framework Implementation

Figure 2 describes a common flow of information and decisions at the following levels within an organization:

- Executive
- Business/Process
- Implementation/Operations

The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into the risk management process, and then collaborates with the implementation/operations level to communicate business needs and create a Profile. The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process and to the implementation/operations level for awareness of business impact.

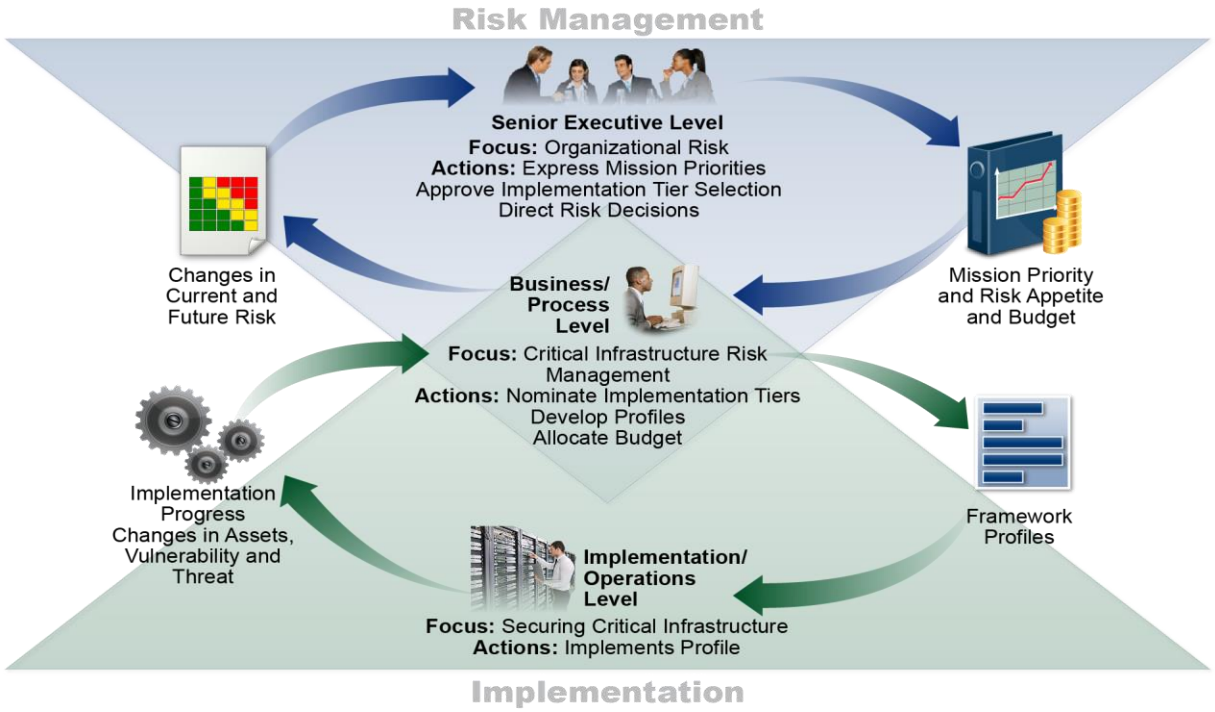


Figure 2: Notional Information and Decision Flows within an Organization

3.0 How to Use the Framework

An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Using the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program. The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization's cybersecurity practices. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

The Framework can be applied throughout the life cycle phases of plan, design, build/buy, deploy, operate, and decommission. The plan phase begins the cycle of any system and lays the groundwork for everything that follows. Overarching cybersecurity considerations should be declared and described as clearly as possible. The plan should recognize that those considerations and requirements are likely to evolve during the remainder of the life cycle. The design phase should account for cybersecurity requirements as a part of a larger multi-disciplinary systems engineering process.[10] A key milestone of the design phase is validation that the system cybersecurity specifications match the needs and risk disposition of the organization as captured in a Framework Profile. The desired cybersecurity outcomes prioritized in a Target Profile should be incorporated when a) developing the system during the build phase and b) purchasing or outsourcing the system during the buy phase. That same Target Profile serves as a list of system cybersecurity features that should be assessed when deploying the system to verify all features are implemented. The cybersecurity outcomes determined by using the Framework then should serve as a basis for ongoing operation of the system. This includes occasional reassessment, capturing results in a Current Profile, to verify that cybersecurity requirements are still fulfilled. Typically, a complex web of dependencies (e.g., compensating and common controls) among systems means the outcomes documented in Target Profiles of related systems should be carefully considered as systems are decommissioned.

The following sections present different ways in which organizations can use the Framework.

3.1 Basic Review of Cybersecurity Practices

The Framework can be used to compare an organization's current cybersecurity activities with those outlined in the Framework Core. Through the creation of a Current Profile, organizations can examine the extent to which they are achieving the outcomes described in the Core Categories and Subcategories, aligned with the five high-level Functions: Identify, Protect, Detect, Respond, and Recover. An organization may find that it is already achieving the desired

[10] NIST Special Publication 800-160 Volume 1, *System Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, Ross et al, November 2016 (updated March 21, 2018), https://doi.org/10.6028/NIST.SP.800-160v1

outcomes, thus managing cybersecurity commensurate with the known risk. Alternatively, an organization may determine that it has opportunities to (or needs to) improve. The organization can use that information to develop an action plan to strengthen existing cybersecurity practices and reduce cybersecurity risk. An organization may also find that it is overinvesting to achieve certain outcomes. The organization can use this information to reprioritize resources.

While they do not replace a risk management process, these five high-level Functions will provide a concise way for senior executives and others to distill the fundamental concepts of cybersecurity risk so that they can assess how identified risks are managed, and how their organization stacks up at a high level against existing cybersecurity standards, guidelines, and practices. The Framework can also help an organization answer fundamental questions, including "How are we doing?" Then they can move in a more informed way to strengthen their cybersecurity practices where and when deemed necessary.

3.2 Establishing or Improving a Cybersecurity Program

The following steps illustrate how an organization could use the Framework to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity.

Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and

Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

An organization repeats the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also use this process to align their cybersecurity program with their desired Framework Implementation Tier.

3.3 Communicating Cybersecurity Requirements with Stakeholders

The Framework provides a common language to communicate requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure products and services. Examples include:

- An organization may use a Target Profile to express cybersecurity risk management requirements to an external service provider (e.g., a cloud provider to which it is exporting data).
- An organization may express its cybersecurity state through a Current Profile to report results or to compare with acquisition requirements.
- A critical infrastructure owner/operator, having identified an external partner on whom that infrastructure depends, may use a Target Profile to convey required Categories and Subcategories.
- A critical infrastructure sector may establish a Target Profile that can be used among its constituents as an initial baseline Profile to build their tailored Target Profiles.
- An organization can better manage cybersecurity risk among stakeholders by assessing their position in the critical infrastructure and the broader digital economy using Implementation Tiers.

Communication is especially important among stakeholders up and down supply chains. Supply chains are complex, globally distributed, and interconnected sets of resources and processes

between multiple levels of organizations. Supply chains begin with the sourcing of products and services and extend from the design, development, manufacturing, processing, handling, and delivery of products and services to the end user. Given these complex and interconnected relationships, supply chain risk management (SCRM) is a critical organizational function.[11]

Cyber SCRM is the set of activities necessary to manage cybersecurity risk associated with external parties. More specifically, cyber SCRM addresses both the cybersecurity effect an organization has on external parties and the cybersecurity effect external parties have on an organization.

A primary objective of cyber SCRM is to identify, assess, and mitigate "products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain[12]." Cyber SCRM activities may include:

- Determining cybersecurity requirements for suppliers,
- Enacting cybersecurity requirements through formal agreement (e.g., contracts),
- Communicating to suppliers how those cybersecurity requirements will be verified and validated,
- Verifying that cybersecurity requirements are met through a variety of assessment methodologies, and
- Governing and managing the above activities.

As depicted in Figure 3, cyber SCRM encompasses technology suppliers and buyers, as well as non-technology suppliers and buyers, where technology is minimally composed of information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT). Figure 3 depicts an organization at a single point in time. However, through the normal course of business operations, most organizations will be both an upstream supplier and downstream buyer in relation to other organizations or end users.

[11] Communicating Cybersecurity Requirements (Section 3.3) and Buying Decisions (Section 3.4) address only two uses of the Framework for cyber SCRM and are not intended to address cyber SCRM comprehensively.

[12] NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Boyens et al, April 2015, https://doi.org/10.6028/NIST.SP.800-161

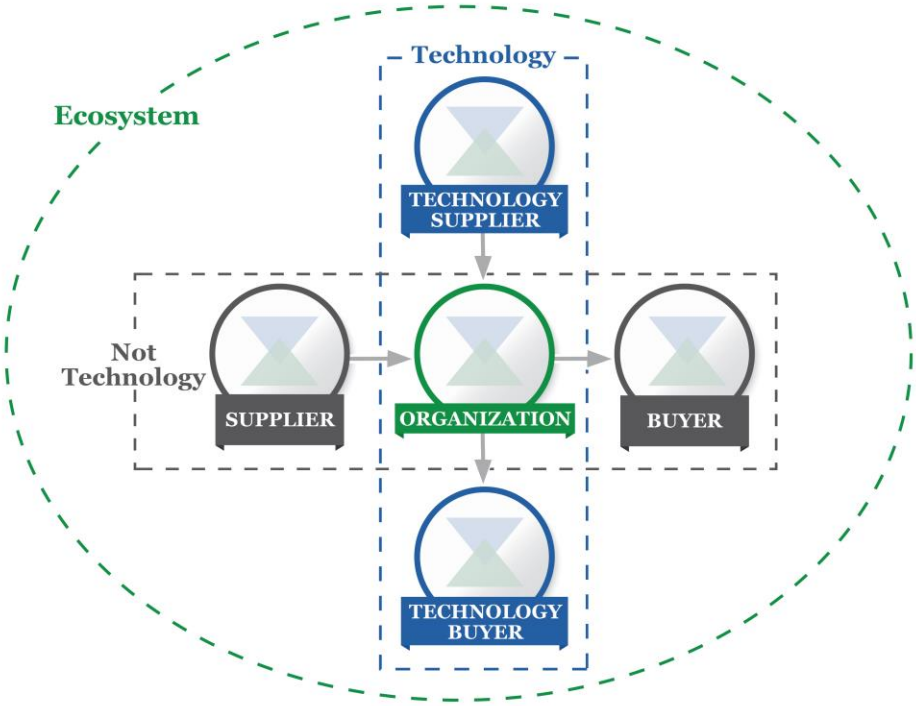


Figure 3: Cyber Supply Chain Relationships

The parties described in Figure 3 comprise an organization's cybersecurity ecosystem. These relationships highlight the crucial role of cyber SCRM in addressing cybersecurity risk in critical infrastructure and the broader digital economy. These relationships, the products and services they provide, and the risks they present should be identified and factored into the protective and detective capabilities of organizations, as well as their response and recovery protocols.

In the figure above, "Buyer" refers to the downstream people or organizations that consume a given product or service from an organization, including both for-profit and not-for-profit organizations. "Supplier" encompasses upstream product and service providers that are used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products or services provided to the Buyer. These terms are applicable for both technology-based and non-technology-based products and services.

Whether considering individual Subcategories of the Core or the comprehensive considerations of a Profile, the Framework offers organizations and their partners a method to help ensure the new product or service meets critical security outcomes. By first selecting outcomes that are relevant to the context (e.g., transmission of Personally Identifiable Information (PII), mission critical service delivery, data verification services, product or service integrity) the organization then can evaluate partners against those criteria. For example, if a system is being purchased that will monitor Operational Technology (OT) for anomalous network communication, availability may be a particularly important cybersecurity objective to achieve and should drive a Technology Supplier evaluation against applicable Subcategories (e.g., ID.BE-4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE.AE-5).

3.4 Buying Decisions

Since a Framework Target Profile is a prioritized list of organizational cybersecurity requirements, Target Profiles can be used to inform decisions about buying products and services. This transaction varies from Communicating Cybersecurity Requirements with Stakeholders (addressed in Section 3.3) in that it may not be possible to impose a set of cybersecurity requirements on the supplier. The objective should be to make the best buying decision among multiple suppliers, given a carefully determined list of cybersecurity requirements. Often, this means some degree of trade-off, comparing multiple products or services with known gaps to the Target Profile.

Once a product or service is purchased, the Profile also can be used to track and address residual cybersecurity risk. For example, if the service or product purchased did not meet all the objectives described in the Target Profile, the organization can address the residual risk through other management actions. The Profile also provides the organization a method for assessing if the product meets cybersecurity outcomes through periodic review and testing mechanisms.

3.5 Identifying Opportunities for New or Revised Informative References

The Framework can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs. An organization implementing a given Subcategory, or developing a new Subcategory, might discover that there are few Informative References, if any, for a related activity. To address that need, the organization might collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards, guidelines, or practices.

3.6 Methodology to Protect Privacy and Civil Liberties

This section describes a methodology to address individual privacy and civil liberties implications that may result from cybersecurity. This methodology is intended to be a general set of considerations and processes since privacy and civil liberties implications may differ by sector or over time and organizations may address these considerations and processes with a range of technical implementations. Nonetheless, not all activities in a cybersecurity program engender privacy and civil liberties considerations. Technical privacy standards, guidelines, and additional best practices may need to be developed to support improved technical implementations.

Privacy and cybersecurity have a strong connection. An organization's cybersecurity activities also can create risks to privacy and civil liberties when personal information is used, collected, processed, maintained, or disclosed. Some examples include: cybersecurity activities that result in the over-collection or over-retention of personal information; disclosure or use of personal information unrelated to cybersecurity activities; and cybersecurity mitigation activities that result in denial of service or other similar potentially adverse impacts, including some types of incident detection or monitoring that may inhibit freedom of expression or association.

The government and its agents have a responsibility to protect civil liberties arising from cybersecurity activities. As referenced in the methodology below, government or its agents that own or operate critical infrastructure should have a process in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements.

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

To address privacy implications, organizations may consider how their cybersecurity program might incorporate privacy principles such as: data minimization in the collection, disclosure, and retention of personal information material related to the cybersecurity incident; use limitations outside of cybersecurity activities on any information collected specifically for cybersecurity activities; transparency for certain cybersecurity activities; individual consent and redress for adverse impacts arising from use of personal information in cybersecurity activities; data quality, integrity, and security; and accountability and auditing.

As organizations assess the Framework Core in Appendix A, the following processes and activities may be considered as a means to address the above-referenced privacy and civil liberties implications:

Governance of cybersecurity risk

- An organization's assessment of cybersecurity risk and potential risk responses considers the privacy implications of its cybersecurity program.
- Individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained.
- Process is in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements.
- Process is in place to assess implementation of the above organizational measures and controls.

Approaches to identifying, authenticating, and authorizing individuals to access organizational assets and systems

- Steps are taken to identify and address the privacy implications of identity management and access control measures to the extent that they involve collection, disclosure, or use of personal information.

Awareness and training measures

- Applicable information from organizational privacy policies is included in cybersecurity workforce training and awareness activities.
- Service providers that provide cybersecurity-related services for the organization are informed about the organization's applicable privacy policies.

Anomalous activity detection and system and assets monitoring

- Process is in place to conduct a privacy review of an organization's anomalous activity detection and cybersecurity monitoring.

Response activities, including information sharing or other mitigation efforts

- Process is in place to assess and address whether, when, how, and the extent to which personal information is shared outside the organization as part of cybersecurity information sharing activities.
- Process is in place to conduct a privacy review of an organization's cybersecurity mitigation efforts.

4.0 Self-Assessing Cybersecurity Risk with the Framework

The Cybersecurity Framework is designed to reduce risk by improving the management of cybersecurity risk to organizational objectives. Ideally, organizations using the Framework will be able to measure and assign values to their risk *along with* the cost and benefits of steps taken to reduce risk to acceptable levels. The better an organization is able to measure its risk, costs, and benefits of cybersecurity strategies and steps, the more rational, effective, and valuable its cybersecurity approach and investments will be.

Over time, self-assessment and measurement should improve decision making about investment priorities. For example, measuring – or at least robustly characterizing – aspects of an organization's cybersecurity state and trends over time can enable that organization to understand and convey meaningful risk information to dependents, suppliers, buyers, and other parties. An organization can accomplish this internally or by seeking a third-party assessment. If done properly and with an appreciation of limitations, these measurements can provide a basis for strong trusted relationships, both inside and outside of an organization.

To examine the effectiveness of investments, an organization must first have a clear understanding of its organizational objectives, the relationship between those objectives and supportive cybersecurity outcomes, and how those discrete cybersecurity outcomes are implemented and managed. While measurements of all those items is beyond the scope of the Framework, the cybersecurity outcomes of the Framework Core support self-assessment of investment effectiveness and cybersecurity activities in the following ways:

- Making choices about how different portions of the cybersecurity operation should influence the selection of Target Implementation Tiers,
- Evaluating the organization's approach to cybersecurity risk management by determining Current Implementation Tiers,
- Prioritizing cybersecurity outcomes by developing Target Profiles,
- Determining the degree to which specific cybersecurity steps achieve desired cybersecurity outcomes by assessing Current Profiles, and
- Measuring the degree of implementation for controls catalogs or technical guidance listed as Informative References.

The development of cybersecurity performance metrics is evolving. Organizations should be thoughtful, creative, and careful about the ways in which they employ measurements to optimize use, while avoiding reliance on artificial indicators of current state and progress in improving cybersecurity risk management. Judging cyber risk requires discipline and should be revisited periodically. Any time measurements are employed as part of the Framework process, organizations are encouraged to clearly identify and know why these measurements are important and how they will contribute to the overall management of cybersecurity risk. They also should be clear about the limitations of measurements that are used.

For example, tracking security measures and business outcomes may provide meaningful insight as to how changes in granular security controls affect the completion of organizational objectives. Verifying achievement of some organizational objectives requires analyzing the data only *after* that objective was to have been achieved. This type of lagging measure is more

absolute. However, it is often more valuable to predict whether a cybersecurity risk *may* occur, and the impact it *might* have, using a leading measure.

Organizations are encouraged to innovate and customize how they incorporate measurements into their application of the Framework with a full appreciation of their usefulness and limitations.

Appendix A: Framework Core

This appendix presents the Framework Core: a listing of Functions, Categories, Subcategories, and Informative References that describe specific cybersecurity activities that are common across all critical infrastructure sectors. The chosen presentation format for the Framework Core does not suggest a specific implementation order or imply a degree of importance of the Categories, Subcategories, and Informative References. The Framework Core presented in this appendix represents a common set of activities for managing cybersecurity risk. While the Framework is not exhaustive, it is extensible, allowing organizations, sectors, and other entities to use Subcategories and Informative References that are cost-effective and efficient and that enable them to manage their cybersecurity risk. Activities can be selected from the Framework Core during the Profile creation process and additional Categories, Subcategories, and Informative References may be added to the Profile. An organization's risk management processes, legal/regulatory requirements, business/mission objectives, and organizational constraints guide the selection of these activities during Profile creation. Personal information is considered a component of data or assets referenced in the Categories when assessing security risks and protections.

While the intended outcomes identified in the Functions, Categories, and Subcategories are the same for IT and ICS, the operational environments and considerations for IT and ICS differ. ICS have a direct effect on the physical world, including potential risks to the health and safety of individuals, and impact on the environment. Additionally, ICS have unique performance and reliability requirements compared with IT, and the goals of safety and efficiency must be considered when implementing cybersecurity measures.

For ease of use, each component of the Framework Core is given a unique identifier. Functions and Categories each have a unique alphabetic identifier, as shown in Table 1. Subcategories within each Category are referenced numerically; the unique identifier for each Subcategory is included in Table 2.

Additional supporting material, including Informative References, relating to the Framework can be found on the NIST website at http://www.nist.gov/cyberframework/.

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 2: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **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 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		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
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative References
		third-party stakeholders (e.g., suppliers, customers, partners) are established	**ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** BAI03.02, DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	**CIS CSC** 19 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 Rev. 4** -1 controls from all security control families

Function	Category	Subcategory	Informative References
	management of cybersecurity risk.	**ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	**CIS CSC** 19 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	**CIS CSC** 19 **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 4** -1 controls from all security control families
		ID.GV-4: Governance and risk management processes address cybersecurity risks	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/IEC 27001:2013** Clause 6 **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**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, RA-3, 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

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

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, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	**CIS CSC** 4 **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and prioritized	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** Clause 6.1.3 **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 **NIST SP 800-53 Rev. 4** PM-9

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative References
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	**COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**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-2: Physical access to assets is managed and protected	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		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

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative References
			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, AC-5, AC-6, AC-14, AC-16, AC-24
		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-6: Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		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

Function	Category	Subcategory	Informative References
			ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Privileged users understand their roles and responsibilities	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	**CIS CSC** 17 **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
		PR.AT-4: Senior executives understand their roles and responsibilities	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	**CIS CSC** 17 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**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
		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
		PR.DS-4: Adequate capacity to ensure availability is maintained	**CIS CSC** 1, 2, 13 **COBIT 5** APO13.01, BAI04.04 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	**CIS CSC** 13 **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 **ISA 62443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4,

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative References
			A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rev. 4** SC-16, SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	**COBIT 5** BAI03.05 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISO/IEC 27001:2013** A.11.2.4 **NIST SP 800-53 Rev. 4** SA-10, SI-7
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3

Function	Category	Subcategory	Informative References
			ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: Configuration change control processes are in place	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI06.01 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested	**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
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	**COBIT 5** BAI09.03, DSS05.06 **ISA 62443-2-1:2009** 4.3.4.4.4 **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.11.2.7 **NIST SP 800-53 Rev. 4** MP-6

Function	Category	Subcategory	Informative References
		PR.IP-7: Protection processes are improved	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared	**COBIT 5** BAI08.04, DSS03.04 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	**CIS CSC** 19 **COBIT 5** APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Response and recovery plans are tested	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	**CIS CSC** 5, 16 **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative References
		PR.IP-12: A vulnerability management plan is developed and implemented	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS05.01, DSS05.02 **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	**COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.7 **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	**CIS CSC** 3, 5 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53 Rev. 4** MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**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
		PR.PT-2: Removable media is protected and its use restricted according to policy	**CIS CSC** 8, 13 **COBIT 5** APO13.01, DSS05.02, DSS05.06 **ISA 62443-3-3:2013** SR 2.3 **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	**CIS CSC** 3, 11, 14 **COBIT 5** DSS05.02, DSS05.05, DSS06.06 **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 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, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	**CIS CSC** 8, 12, 15 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	**COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 **ISA 62443-2-1:2009** 4.3.2.5.2 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected	**DE.AE-1:** A baseline of network operations and expected data flows for	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3

Function	Category	Subcategory	Informative References
	and the potential impact of events is understood.	users and systems is established and managed	**ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Incident alert thresholds are established	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

Function	Category	Subcategory	Informative References
	the effectiveness of protective measures.	**DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events	**COBIT 5** DSS01.04, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2 **ISO/IEC 27001:2013** A.12.2.1 **NIST SP 800-53 Rev. 4** SI-3, SI-8
		DE.CM-5: Unauthorized mobile code is detected	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4 **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	**COBIT 5** APO07.06, APO10.05 **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed	**CIS CSC** 4, 20

Function	Category	Subcategory	Informative References
			COBIT 5 BAI03.10, DSS05.01 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	**CIS CSC** 19 **COBIT 5** APO01.02**,** DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2 **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: Detection processes are tested	**COBIT 5** APO13.02, DSS05.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Event detection information is communicated	**CIS CSC** 19 **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Incidents are reported consistent with established criteria	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	**CIS CSC** 19 **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative References
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained	**CIS CSC** 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: Incidents are mitigated	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	**COBIT 5** APO12.06, BAI05.07, DSS04.08 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative References
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
		RC.CO-2: Reputation is repaired after an incident	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Clause 7.4
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4

Information regarding Informative References described in Appendix A may be found at the following locations:

- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): https://www.cisecurity.org
- American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
- ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements*: https://www.iso.org/standard/54534.html
- NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (including updates as of January 22, 2015). https://doi.org/10.6028/NIST.SP.800-53r4. Informative References are only mapped to the control level, though any control enhancement might be found useful in achieving a subcategory outcome.

Mappings between the Framework Core Subcategories and the specified sections in the Informative References are not intended to definitively determine whether the specified sections in the Informative References provide the desired Subcategory outcome.

Informative References are not exhaustive, in that not every element (e.g., control, requirement) of a given Informative Reference is mapped to Framework Core Subcategories.

Appendix B: Glossary

This appendix defines selected terms used in the publication.

Table 3: Framework Glossary

Buyer	The people or organizations that consume a given product or service.
Category	The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Identity Management and Access Control," and "Detection Processes."
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.
Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks.
Cybersecurity Event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
Cybersecurity Incident	A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the "Cybersecurity Framework."
Framework Core	A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.
Framework Implementation Tier	A lens through which to view the characteristics of an organization's approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.

Framework Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.
Function	One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify, Protect, Detect, Respond, and Recover.
Identify (function)	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Informative Reference	A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory. An example of an Informative Reference is ISO/IEC 27001 Control A.10.8.3, which supports the "Data-in-transit is protected" Subcategory of the "Data Security" Category in the "Protect" function.
Mobile Code	A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.
Protect (function)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Privileged User	A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Recover (function)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
Respond (function)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Risk	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.
Risk Management	The process of identifying, assessing, and responding to risk.
Subcategory	The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."

Supplier	Product and service providers used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products of services provided to that organization's Buyers.
Taxonomy	A scheme of classification.

Appendix C: Acronyms

This appendix defines selected acronyms used in the publication.

ANSI	American National Standards Institute
CEA	Cybersecurity Enhancement Act of 2014
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technology
CPS	Cyber-Physical Systems
CSC	Critical Security Control
DHS	Department of Homeland Security
EO	Executive Order
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IoT	Internet of Things
IR	Interagency Report
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
OT	Operational Technology
PII	Personally Identifiable Information
RFI	Request for Information
RMP	Risk Management Process
SCRM	Supply Chain Risk Management
SP	Special Publication

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018