7. Reporting

7.1 Integrated Data Collection (IDC)

The IDC is the OMB Office of the Federal CIO's (OFCIO) quarterly reporting mechanism to capture data and information related to PortfolioStat, DCOI, and other OFCIO-led initiatives. Agencies determine the individuals responsible for IDC reporting and tend to include a team of individuals from across an agency with a leader who reports to the CIO, Deputy CIO, or CISO. These individuals for each agency can be found in the IDC section of MAX.gov.[316]

OFCIO established the Information Collection Review Board (ICRB)[317] to manage the IDC process on a quarterly basis and make any necessary changes to the reporting instructions. The ICRB ensures that the IDC process is efficient and gathers relevant data while limiting the burden on participating agencies[318].

Each quarter, OFCIO produces the Quarterly IDC Instructions that documents reporting fields and requirements. OFCIO also solicits feedback from reporting agencies and partners to improve the reporting process and remove unnecessary data collections when appropriate. The "Quarter-By Quarter IDC Timeline & Changes" table on MAX.gov collects from the May 2018 IDC quarter and each quarter thereafter, new engagements related to any agency-led TechStats, OMB-led TechStats, or OMB engagements like PortfolioStats; information regarding past engagements; and reporting on any agreed-upon action items resulting from those sessions.[319]

For more information consult the Reporting Calendar.

7.2 CPIC Reporting

The CPIC reporting process includes all stages of capital programming including planning, budgeting, procurement, management, and assessment. OMB's reporting requirements are communicated to federal executive departments and agencies through the annual updates to OMB Circular A-11, Section 55.[320] CIOs are expected to coordinate to ensure that IT budget data is consistent with the agency's budget submission and are also expected to provide a CIO Evaluation Report for all Major Investments and Part 3 Standard Investments. Agency CPIC information is collected through the annual E-Gov MAX collection, which includes the collection of IT investment information for the Previous Year's (PY) actual spend, Current Year (CY) estimated spend, and requested spend in the President's Budget request for the Budget Year (BY). The CPIC reporting process heavily leverages the TBM framework to gain increased granularity about IT spend across federal executive departments and agencies.[321]

[316] The website MAX.gov is only accessible to federal employees.

[317] OMB. E-Gov Integrated Data Collection (IDC). https://community.max.gov/x/LhtGJw

[318] Participation varies by reporting activity. See subsequent sections for agency requirements.

[319] OMB. E-Gov Integrated Data Collection (IDC). Attachments. Quarterly IDC Instructions November 2020. https://community.max.gov/pages/viewpage.action?pageId=658905902

[320] CIO Council. Capital Planning and Investment Control (CPIC). https://www.cio.gov/policies-and-priorities/cpic/

[321] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. 2020. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

Agencies are no longer required to submit an IT Resources Statement as part of their agency budget submission to OMB. Other IT related materials are required, as detailed in Section 55, and submitted according to the following IT CPIC Milestones:

- August
  - Draft Agency IT Investment Portfolio Summary submission
  - Verification that the required E-Gov/Line of Business (LoB) contribution levels are being included in the agency's budget plans
- September
  - Agency IT Portfolio Summary submission
  - Agency IT Portfolio Summary Details
- January
  - Final Agency IT Portfolio Summary and IT Portfolio Summary Details based on the President's Budget submissions
- June
  - Optional Mid-Session Review submission

To the extent possible, align budget accounts with programs, distinguishing among components that contribute to different strategic objectives.[322]

For more information consult the Reporting Calendar.

7.3 DCOI Reporting

DCOI reporting is performed through three methods: a data center inventory reported to OMB quarterly, a DCOI strategic plan updated annually, and a list of FITARA milestones updated quarterly.[323] These submissions are expected to be submitted under the direction of the CIO. Additionally, agency-reported public data can be viewed on the IT Dashboard.[324]

The Data Center Inventory involves the quarterly submission of data containing the full inventory of data centers by CFO-Act agencies to OMB for data center and DCOI implementation oversight. This inventory is collected as a part of the IDC and is generally collected for Q1 by the end of February, Q2 by the end of May, Q3 by the end of August, and Q4 by the end of November, though specific dates may vary.[325]

The DCOI Strategic Plan is required as a part of FITARA and involves the annual publication of strategic plans describing the agency’s consolidation and optimization strategy. The strategic plan publications each year is reported as a part of the Q2 IDC process for that year and should be published at “[agency].gov/digitalstrategy” in the Data Center Optimization Initiative Strategic Plans category.[326]

[322] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. Section 51. 2020. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

[323] OMB. DCOI - Reporting. https://datacenters.cio.gov/reporting/

[324] OMB. IT Dashboard. https://itdashboard.gov/

[325] OMB. E-Gov Integrated Data Collection (IDC). https://community.max.gov/x/LhtGJw

[326] OMB. Implementation Guidance - FITARA. DCOI Strategic Plan Schema. https://management.cio.gov/schema/#DCOI

Furthermore, agencies are also required to identify at least five FITARA milestones per fiscal year to be achieved through DCOI. These milestones should be published at “[agency].gov/digitalstrategy/FITARAmilestones.json'' and should be updated quarterly as progress is achieved and then reviewed in PortfolioStat sessions.[327]

For more information consult the Reporting Calendar.

7.4 FISMA Reporting

FISMA metrics are aligned to the five functions outlined in NIST’s Framework for Improving Critical Infrastructure and Cybersecurity: Identify, Protect, Detect, Respond, and Recover. Annually, OMB releases a memorandum establishing FISMA reporting guidance and deadlines with additional details provided through CyberScope and MAX.[328] FISMA documents are available on the cisa.gov website for each fiscal year of FISMA, while the memorandums are available on the whitehouse.gov website.[329]

Typically, the memorandum is released around October or November for the upcoming fiscal year, see OMB M-20-04 for the FY20 guidance.[330] The memorandum will also specify the reported performance metrics with any Cross Agency Priorities (CAP), as well as provide instructions on report content and details for the development of annual agency FISMA reports. Typical CAP metrics include specific metrics around the categories of Information Security Continuous Monitoring, Identify and Credential Access Management, Anti-Phishing and Malware Defense.

FISMA data is assessed both quarterly and annually. Quarterly, as mandated by OMB and the NSC, agencies are required to collect FISMA performance metrics data and upload the results into CyberScope. This collection typically involves multiple persons working with the responsible POC and is then reviewed by the CISO and CIO prior to being uploaded. The Annual FISMA Report typically consists of three main sections:

- CIO: Implementation of FISMA CAP measures and base measures
- SAOP: Implementation of a Privacy Program in compliance with the Privacy Act
- IG: Questions about security and privacy programs independently answered by the agency IG

Typically, these sections will be completed by the relevant teams within agencies, incorporated into the annual report, reviewed, and then are required to be approved and signed by the head of the agency. Additionally, agencies may also use this time to conduct a FISMA self-assessment to assess and support their FISMA compliance.

[327] OMB. Implementation Guidance - FITARA. https://management.cio.gov/

[328] GSA. FISMA Implementation Guide. CIO-IT Security-04-26. 4/16/2019. https://www.gsa.gov/cdnstatic/FISMA_Implementation_Guide_%5BCIO-IT_Security-04-26_Rev2%5D_04-16-2019.pdf

[329] CISA. Federal Information Security Modernization Act. https://www.cisa.gov/federal-information-security-modernization-act

[330] OMB M-20-04. Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements. 11/19/2019. https://www.whitehouse.gov/wp-content/uploads/2019/11/M-20-04.pdf

Finally, the annual report is also required to be submitted to the Chairperson and Ranking Member of the House Committee on Oversight and Government Reform, the House Committee on Homeland Security, the House Committee on Science, Space, and Technology, the Senate Committee on Homeland Security and Government Affairs, the Senate Committee on Commerce, Science, and Transportation, the appropriate authorization and appropriations committees in both the House and Senate, as well as to the GAO and to the Comptroller General of the United States. For more information consult the Reporting Calendar.

7.5 FITARA Reporting

FITARA requires federal agencies to submit annual reports that include:

- Comprehensive data center inventories,
- Multiyear strategies to consolidate and optimize data centers,
- Performance metrics and a timeline for agency action, and
- Yearly calculations of investment and cost savings related to FITARA implementation.[331]

See FITARA section for more information.

7.6 FISMA Report to Congress

OMB publishes a FISMA Annual Report to Congress[332] each fiscal year which includes data reported by agencies to OMB and CISA highlighting government-wide cybersecurity programs and initiatives, and agencies' progress to enhance federal cybersecurity from the past year and into the future. Part of what is included in agencies' evaluations submitted to OMB include independent evaluations by the IG or independent external auditor for each agency which determines the effectiveness of the information security policies, procedures, and practices supporting their agency's information security programs.[333] The FISMA Annual Report to Congress can be found at www.whitehouse.gov.

For more information consult the Reporting Calendar.

[331] Congressional Research Service. The Current State of Federal Information Technology Acquisition Reform and Management. 2/03/2020. https://fas.org/sgp/crs/misc/R44843.pdf

[332] The White House. Federal Information Security Modernization Act of 2014. Annual Report to Congress. FY 2018. https://www.whitehouse.gov/wp-content/uploads/2019/08/FISMA-2018-Report-FINAL-to-post.pdf

[333] GAO-19-545. Agencies and OMB Need to Strengthen Policies and Practices. July 2019. https://www.gao.gov/assets/710/700588.pdf

8. Reporting Calendar

Federal agencies are required by OMB to participate in several reporting activities for the planning, programming, management, and execution of IT. The following Reporting Calendar outlines those reporting activities and the periods for which they take place during the year.

January

- CPIC Final Submission (after budget pass-back)
- Q1 CIO FISMA Reporting
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

February

- Quarterly Integrated Data Collection Submissions
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

March

- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

April

- Q2 CIO FISMA Reporting
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

May

- Annual Data Center Optimization Initiative Strategic Plan Update
- Quarterly Integrated Data Collection Submissions
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

June

- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

July

- Q3 CIO FISMA Reporting
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

August

- Quarterly Integrated Data Collection Submissions
- CPIC Test
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

September

- CPIC Submission
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

October

- Annual CIO, IG, and SAOP FISMA Reporting
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

November

- Quarterly Integrated Data Collection Submissions
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

December

- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

9. Additional Resources

9.1 CIO Council Resources

Report to the President on Federal IT Modernization

In May 2017, President Trump issued Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,[334] which commissioned the Federal IT Modernization Report to describe the legal, policy, and budgetary considerations around federal network architectures and provide recommendations to improve security, make Federal IT more agile and responsive, and make infrastructure more cost effective.

The Report to the President on Federal IT Modernization[335] was produced in December 2017 and outlines the White House's American Technology Council and the Office of Science and Technology Policy's vision and recommendations to modernize citizen-facing services. The report incorporates feedback from more than 100 companies and individuals, as well as extensive input from agencies and IT policy experts throughout the federal government.

The report chiefly recommended network modernization and consolidation, a shift toward shared services to enable future network architectures, and providing additional resources for federal network IT modernization. All recommendations made in the report were to be completed no more than 365 days after publication, and there are not current, ongoing requirements. The report heavily influenced the PMA, which established the White House's 2018 priorities.[336]

Application Rationalization Playbook

In collaboration with OMB and GSA, the Application Rationalization Playbook[337] was developed and finalized in June 2019 by the Federal CIOC in support of the Federal Cloud Computing Strategy,[338] also known as "Cloud Smart". It was designed for IT Portfolio Managers to consider their agency's approach to IT modernization. Additional guidance and policies germane to application rationalization include: the Federal IT Modernization Report[339] which was issued in December 2017; EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure which was issued in May 2017; and Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing which was issued by OMB as Memorandum M-16-12.

[334] Executive Order 13800. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 5/11/2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[335] CIO Council. Report to the President on Federal IT Modernization. December 2017. https://www.cio.gov/assets/resources/Report-to-the-President-on-IT-Modernization-Final.pdf

[336] The White House. President's Management Agenda. April 2018. https://www.performance.gov/PMA/Presidents_Management_Agenda.pdf

[337] CIO Council. The Application Rationalization Playbook. https://www.cio.gov/assets/files/Application-Rationalization-Playbook.pdf

[338] OMB. Federal Cloud Computing Strategy. https://cloud.cio.gov/strategy/

[339] CIO Council. Report to the President on Federal IT Modernization. December 2017. https://www.cio.gov/assets/resources/Report-to-the-President-on-IT-Modernization-Final.pdf

Application rationalization helps federal agencies mature IT portfolio management capabilities, empower leaders to make informed decisions, and improve the delivery of key mission and business services. It requires buy-in from stakeholders across the enterprise, including senior leaders, technology staff members, cybersecurity experts, business leads, financial practitioners, acquisition and procurement experts, and end user communities. Rationalization efforts rely on leadership support and continual engagement with stakeholders to deliver sustainable change. The playbook addresses challenges and opportunities for IT leaders, managers, and technical practitioners, and offers suggestions on how to overcome structural, logistical, and other significant barriers to success.

SOFIT

In January 2017, the CIOC released the State of Federal IT (SOFIT) report, which provided a comprehensive examination of the successes and challenges facing the Federal IT policy landscape. In addition, it provides recommendations on a variety of initiatives in order to improve Federal IT.

Future of the Federal IT Workforce Update

Drawing upon the workforce-related CAP Goals in the PMA, and building on the success of SOFIT, the CIOC undertook a similar examination of the Federal IT workforce and developed the Future of the Federal IT Workforce Update[340] report in May 2020 as an update to SOFIT.

The update is organized around five Primary Issue Areas (PIAs) which form the essential actions required to build an IT workforce for the future. Each PIA is dependent upon the others, and together they form the pillars of a modern, adaptable, and effective Federal IT workforce.

- **Recruit/Hire:** As an increasing number of Federal employees near retirement eligibility, it is essential that Government is able to quickly and efficiently recruit and hire the best IT talent in order to adapt to constantly evolving technologies.
- **Retain:** Government will need to offer its IT workforce opportunities for growth, access to cutting-edge technological tools, and rewards for high performance so they will want to continue to serve agency missions and the public good.
- **Reskill:** Agency-specific and Governmentwide training opportunities will keep IT workers flexible and adaptable in order to keep up with both the pace of innovation and changes that will continue to disrupt the way we conduct work.
- **Augment:** The Federal IT workforce must continue to be supported by agile, flexible groups from both within Government and the private sector, providing surge capacity, access to expertise in cutting-edge process improvements, and emerging or highly specialized technological capabilities.
- **Measure:** Without sufficient qualitative and quantitative data, it will be impossible to gauge successes. Opportunities to leverage data will be identified in order to chart the best path forward by providing a focus on measuring alongside each of the other PIAs.

[340] CIO Council. Future of the Federal IT Workforce Update. May 2020. https://www.cio.gov/assets/resources/Future_of_Federal_IT_Workforce_Update_Public_Version.pdf

The Drivers of the Future of the IT Workforce underpin each of the PIAs. The PIAs must be examined in the light of every driver and the roles these drivers play in shaping the workforce. The considerations for each driver of the future can be described as follows:

- **Innovation:** The increasing pace of technological change is constantly impacting the modern workplace. Recent years have seen changes ranging from the adoption of new programming languages and cloud-based applications to paradigm shifts in emerging technologies, such as robotic process automation and machine learning. Additional training and collaboration opportunities will enable the IT workforce to be flexible enough to adapt to these changes, enabling agencies to execute their missions.
- **Mobility:** Increased flexibility in all of the PIAs will allow the Federal Government to adapt to the workforce of the future. This includes providing vertical career mobility and rewarding high performers, as well as horizontal career mobility opportunities such as reskilling, detailing, and industry exchange programs.
- **Cybersecurity:** All IT work requires some degree of security knowledge and protections, from basic sharing of unclassified documents to defending the nation's most critical IT assets. As such, a skilled and qualified IT workforce is needed to manage an increasingly complex array of security policies and tools to mitigate evolving threats.
- **Collaboration:** As the world grows increasingly more interconnected, so must the Federal IT workforce. This includes coordinating across agencies and cross-functional teams. With the rise of regional offices and improved telework technologies, a more geographically dispersed workforce can now be productive over vast physical distances.
- **Agility:** The Federal Government needs to adapt and scale its use of technology more quickly than ever before. In addition to utilizing agile development methodology and continuous improvement, processes and procedures must also minimize downtime and be adaptable to changing circumstances and expectations in the workforce.

CISO Handbook

This handbook gives CISOs an overview of their roles and responsibilities in relation to Federal cybersecurity. It highlights laws, policies, tools, and initiatives that can be used to create or amend cybersecurity programs.[341]

This handbook aims to:

- Educate and inform new and existing CISOs about their role in successfully implementing Federal cybersecurity;
- Provide resources to help CISOs responsibly apply risk management principles to help Federal agencies meet mission objectives; and
- Make CISOs aware of laws, policies, tools, and initiatives that can assist them as they develop or improve cybersecurity programs for their organizations.

[341] CIO Council. Guidance for Chief Information Security Officers (CISO). https://www.cio.gov/resources/ciso-handbook/

9.2 NIST Resources

NIST Risk Management Framework (RMF)
The NIST RMF[342] provides a foundational process that integrates security and risk management activities into the system development life cycle and brings many of the NIST documents together into an overall approach to managing risk. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations.[343]

CIOs must conduct program portfolio reviews as part of CPIC to ensure that all programs and the CIO are meeting the requirements of FITARA. This includes a CIO evaluation report to OMB for major IT investments that relate to mission delivery and mission support services investments and standard IT services investments that pertain to IT infrastructure, IT security, and IT management investments. However, CIO evaluations can also be provided for other investment types at the CIOs discretion.

NIST Publications
NIST publishes and creates archives of standards, guidelines, recommendations, and research relating to the security and privacy of information and information systems.

Some examples include:

- Federal Information Processing Standards (FIPS) – FIPS establish mandatory requirements for information processing.
- NIST Special Publications (SPs) – SPs provide guidance for developing agency-wide information security programs, including guidelines, technical specifications, recommendations, and reference materials. NIST SPs comprise multiple sub-series:
  - The NIST SP 800-series focuses on computer security, and
  - The NIST SP 1800-series provides cybersecurity practice guides.
- NIST Internal or Interagency Reports (NISTIRs) – NISTIRs are reports of research findings, including background information for FIPS and SPs.
- NIST Information Technology Laboratory Bulletins (ITL Bulletins) – ITL Bulletins are monthly overviews of NIST's security and privacy publications, programs, and projects.

NIST Cybersecurity Framework (CSF)
The NIST CSF is a tool originally developed for the private sector that agencies must implement to manage cybersecurity risk in accordance with Executive Order 13800. The CSF can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program.

An organization can use the CSF as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. It can help an organization determine which activities are most important to critical service delivery, prioritize expenditures and maximize the impact of investment. The CSF is designed to complement existing business and cybersecurity operations. It provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in

[342] NIST. Risk Management Framework (RMF) Overview. https://csrc.nist.gov/projects/risk-management/rmf-overview
[343] Ibid.

an organization's cybersecurity practices. It also provides a general set of processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

The CSF consists of three parts: the CSF Core, the CSF Profile and the CSF Implementation Tiers. The CSF Core is a set of cybersecurity activities, outcomes and informative references that are common across organizations, providing detailed guidance for developing individual organizational profiles. CSF Profiles help the organization align its cybersecurity activities with its business requirements, risk tolerances and resources. The CSF Implementation Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

Figure 2, Notional Information and Decision Flows within an Organization,[344] describes a common flow of information and decisions at the executive, business/process, and implementation/operations levels within an organization.

OMB and DHS have organized the CIO FISMA metrics around the Cybersecurity Framework, leveraging it as a standard for managing and reducing cybersecurity risks and using the core functions to organize the information agencies must submit.

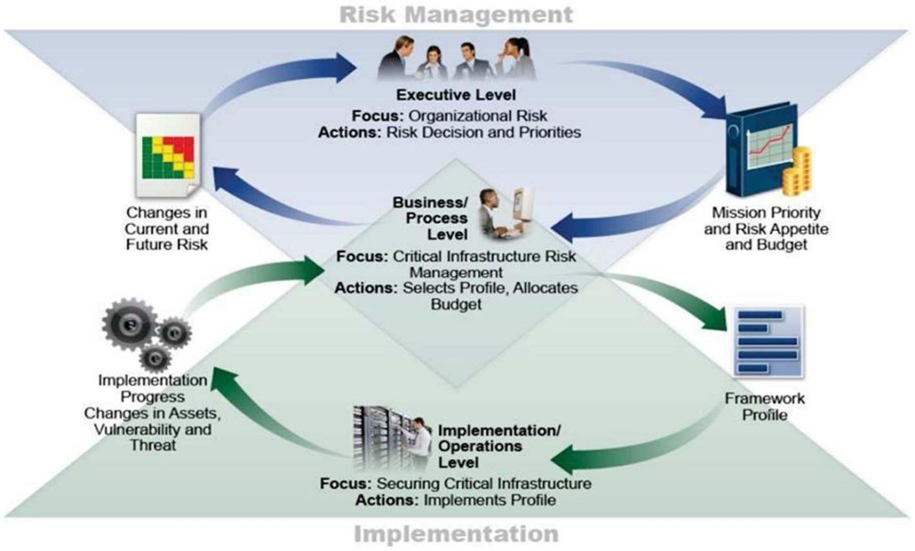
Risk Management
Executive Level
Focus: Organizational Risk
Actions: Risk Decision and Priorities
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget
Implementation Progress Changes in Assets, Vulnerability and Threat
Framework Profile
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

Figure 2: Notional Information and Decision Flows within an Organization

National Initiative for Cybersecurity Education (NICE) Framework

The NICE Cybersecurity Workforce Framework (NICE Framework)[345] is led by NIST at the DOC. The NICE Framework serves as a guide with a collection of common language, classifications, and vocabulary to describe cybersecurity activities and employees. It is meant for a variety of audiences including employers, current and prospective jobs holders, and academic advisors.

[344] NIST. Framework for Improving Critical Infrastructure Cybersecurity. Page. 12. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[345] US-CERT. NICE Cybersecurity Workforce Framework. https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

The NICE Framework includes the following:

- Categories (7)
    - A high-level cluster of common cybersecurity functions
- Specialty Areas (33)
    - Specific areas of cybersecurity work
- Work Roles (52)
    - Detailed lists of cybersecurity work necessary for someone to be aware of to fulfill a job function
- Capability Indicators
    - Combines education, certification, training, experiential learning and continuous learning useful to help someone succeed in a role[346]

9.3 DHS Resources

National Initiative for Cybersecurity Careers and Studies (NICCS)
NICCS, an official website of CISA, is an online resource for cybersecurity training. The courses in the training catalog are cybersecurity focused and delivered by accredited universities, National Centers of Academic Excellence, federal agencies, and other training providers. Each course is mapped to the National Cybersecurity Workforce Framework, the foundation of the National Initiative for Cybersecurity Education (NICE) effort to standardize the cybersecurity field.[347]

Federal Virtual Training Environment (FedVTE)
The FedVTE provides free online cybersecurity training to federal, state, local, tribal, and territorial (SLTT) government employees, federal contractors, US military veterans and the public. Managed by DHS, FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis.[348]

Training, as referred to in the Future of the Federal IT Workforce Update[349] report, is a fundamental component of reskilling opportunities within the Federal Government and helps further the goal of enhancing the national cybersecurity posture. By ensuring that all IT workers have cybersecurity training that is broad enough to at least cover the basics of good cyber hygiene, the potential decreases for breaches to occur through phishing attacks or the introduction of malware.

Register for FedVTE training at https://fedvte.usalearning.gov/.

FISMA Metrics
Each year, three sets of FISMA metrics are developed and used to evaluate the performance of agency cybersecurity and privacy programs.

[346] Ibid.

[347] US-CERT. Learn about NICCS. https://niccs.us-cert.gov/about-niccs/learn-about-niccs

[348] US-CERT. Federal Virtual Training Environment (FedVTE). https://niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte

[349] CIO Council. Future of the Federal IT Workforce Update. May 2020. https://www.cio.gov/assets/resources/Future_of_Federal_IT_Workforce_Update_Public_Version.pdf

1. FISMA CIO metrics are developed by OMB and DHS in close coordination with members of the CIO and CISO Communities and assess the degree to which agencies have implemented certain cybersecurity-related policies and capabilities. CFO Act agencies report this information on a quarterly basis, and non-CFO Act agencies report this information twice annually. These metrics ensure demonstrable progress from agencies' in implementing the Administration's priorities and best practices.
2. FISMA IG metrics are developed by the CIGIE, in collaboration with OMB and DHS, and are used to provide the independent assessment required under FISMA.
3. FISMA SAOP metrics are used to assess the maturity of agency privacy programs. Both the FISMA IG and FISMA SAOP metrics are collected on an annual basis and, along with the fourth quarter FISMA CIO metrics, are reported in the Annual FISMA Report.[350]

FISMA metrics from the current and previous years can be found at CISA.gov for FISMA documents.

9.4 GSA Resources

Highly Adaptive Cybersecurity Services (HACS) Special Item Numbers (SINs)
GSA, in collaboration with DHS and OMB, developed the Highly Adaptive Cybersecurity Services (HACS) Special Item Numbers (SINs) to make it easier for agencies to procure quality cybersecurity services.[351]The program is designed to provide government organizations with access to cybersecurity vendors and to meet the IT security requirements outlined in OMB M-19-03,[352] M-17-12,[353] and the CISO Handbook.[354] They are available through the Multiple Award Schedule (MAS) IT procurement process.

The scope of HACS SINs includes five categories of cybersecurity services for which vendors in the GSA eLibrary have passed a technical evaluation for the categories:

- High Value Asset Assessments
    - Risk and Vulnerability Assessments (RVA)
    - Security Architecture Review (SAR)
    - Systems Security Engineering (SSE)
- RVA
- Cyber Hunt
- Incident Response

[350] CIO Council. CISO Handbook. Page 25. https://www.cio.gov/assets/resources/CISO_Handbook.pdf
[351] GSA. IT Security: GSA's Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SIN). https://interact.gsa.gov/document/it-security-gsas-highly-adaptive-cybersecurity-services-hacs-special-item-number-sin
[352] OMB M-19-03. Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program. 12/10/2018. https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf
[353] OMB M-17-12. Preparing for and Responding to a Breach of Personally Identifiable Information. 1/3/2017. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf
[354] CIO Council. Guidance for Chief Information Security Officers (CISO). https://www.cio.gov/resources/ciso-handbook/

- Penetration Testing[355]

To purchase HACS solutions through the MAS IT procurement process, see the link to the GSA website which includes a HACS Ordering Guide, the HACS SIN vendor listing on the GSA eLibrary, available experts to advise federal agencies on HACS procurement, as well as materials for state and local government ordering and sample Statement of Work (SOW) and Request for Quote (RFQ) Templates.

9.5 OPM Resources

Hiring Guidance

As outlined in the Future of the Federal IT Workforce Report, inefficiencies in the hiring process has contributed to the Federal government's struggle to bring in talent to the IT workforce in a timely and efficient manner. For example, average times to hire are between 110-170 days based on security clearance level, which is four times longer than in industry.[356] As noted by GAO, these struggles have led to challenges in recruiting and retaining CIOs and IT personnel.[357] In order to bring in skilled IT talent, agency CIOs have increasingly used Special Hiring Authorities, such as Schedule A, to meet specific hiring needs that have not been met by the regular hiring process.

Schedule A has been repeatedly granted by OPM for the hiring of digital services staff working on IT projects for the past several fiscal years but has been limited to Modernization, Smarter IT Delivery, and cloud migration projects. An additional hiring flexibility was released by OPM in October 2018 to meet critical technical and cybersecurity needs; this guidance provides direct hire authorities for a variety of STEM and cybersecurity positions.

OPM's most recent regulation was released in April 2019 as the Delegation of Direct-Hire Appointing Authority for IT Positions[358] which builds on the PMA and EO 13833 and provides two CIO direct hire authorities: one for a severe shortage of candidates, and one for a critical hiring need. Both of these authorities provide for an appointment lasting up to four years with an additional four-year appointment at the agency's discretion. This direct hire authority (DHA) expands agencies' ability to maximize DHA for meeting critical IT hiring challenges beyond the government-wide DHA for IT, which is limited to IT positions related to information security.

Federal Employee Viewpoint Survey (FEVS)

FEVS is administered annually by OPM and is a voluntary survey of all permanent federal employees. The survey was initially administered bi-annually as the Federal Human Capital Survey (FHCS) beginning in 2002 and has been administered in its current form since 2010. The survey measures employees' perceptions of whether, and to what extent, conditions characteristic of successful organizations are

[355] GSA. Highly Adaptive Cybersecurity Services (HACS). https://www.gsa.gov/technology/technology-products-services/it-security/highly-adaptive-cybersecurity-services-hacs

[356] CIO Council. Future of the Federal IT Workforce Update. May 2020. https://www.cio.gov/assets/resources/Future_of_Federal_IT_Workforce_Update_Public_Version.pdf

[357] GAO-19-723T. Talent Management Strategies to Help Agencies Better Compete in a Tight Labor Market. 9/25/2019. https://www.gao.gov/assets/710/701649.pdf

[358] OPM. Delegation of Direct-Hire Appointing Authority for IT Positions. 4/5/2019. https://www.chcoc.gov/content/delegation-direct-hire-appointing-authority-it-positions