07

SECTION

REPORTING & REPORTING CALENDAR

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