RECOMMENDATIONS FOR EVOLVING THE FITARA SCORECARD

A Report Developed by the American Council for Technology-Industry Advisory Council (ACT-IAC)

September 14, 2022

American Council for Technology-Industry Advisory Council (ACT-IAC)

The American Council for Technology-Industry Advisory Council (ACT-IAC) is a non-profit educational organization established to accelerate government mission outcomes through collaboration, leadership and education. ACT-IAC provides a unique, objective, and trusted forum where government and industry executives are working together to improve public services and agency operations through the use of technology. ACT-IAC contributes to better communication between government and industry, collaborative and innovative problem solving, and a more professional and qualified workforce. The information, conclusions, and recommendations contained in this publication were produced by volunteers from government and industry who share the ACT-IAC vision of a more effective and innovative government. ACT-IAC volunteers represent a wide diversity of organizations (public and private) and functions. These volunteers use the ACT-IAC collaborative process, refined over forty years of experience, to produce outcomes that are consensus-based. For additional information, visit the ACT-IAC website at www.actiac.org .

American Council for Technology-Industry Advisory Council (ACT-IAC)
3040 Williams Drive, Suite 500, Fairfax, VA 22031
www.actiac.org ● (p) (703) 208.4800 (f) ● (703) 208.4805
Accelerating Government Mission Outcomes Through Collaboration, Leadership and Education

Table of Contents

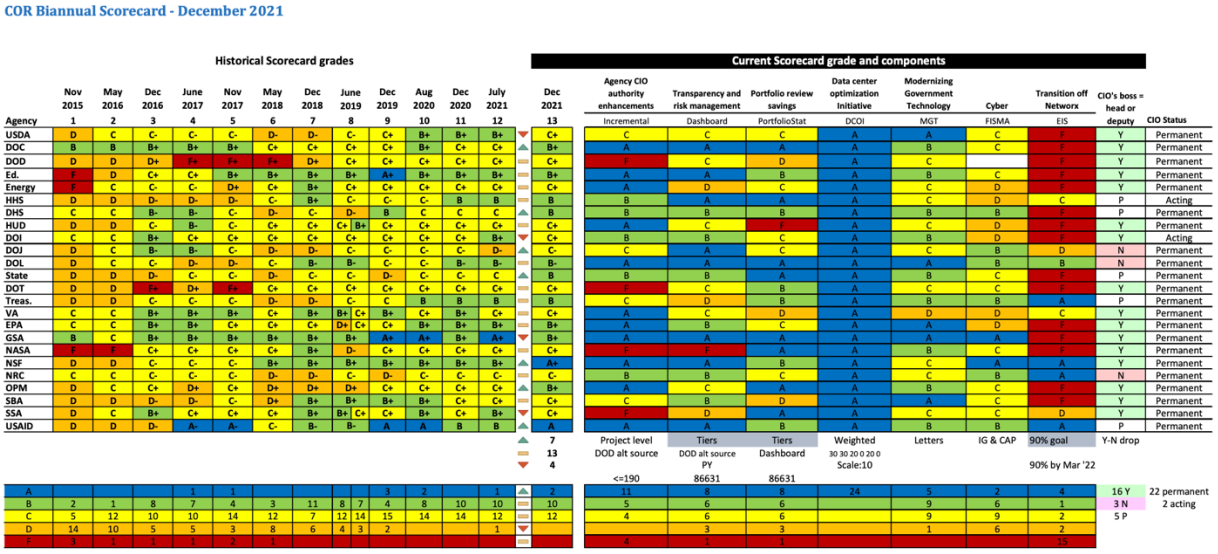
Introduction

FITARA has had a significant positive impact on agencies. While the FITARA legislation is valuable, the consistent oversight from Congress has made a real difference, especially the use of the FITARA Scorecard to spotlight the efforts, or lack thereof, of agencies to advance IT management in those areas in which the Scorecard measures progress. As was presented and discussed in the FITARA 13.0 Hearing in January of 2022, there is consensus that the FITARA Scorecard should evolve to encompass the evolution of agency infrastructure and to make it even more of a valuable tool in measuring an agency's IT management maturity of its unclassified systems environment.

The American Council for Technology – Industry Advisory Council (ACT-IAC) created a project team of former senior government IT leaders, all of whom have had significant past involvement in FITARA. The project team consists of individuals with policy, management, operational, and legislative backgrounds—thus ensuring the project team considered various viewpoints when developing recommendations to evolve the FITARA Scorecard. More information on the project team can be found in the Appendix.

The recommendations contained in this report are based on the project team's consensus view regarding those changes that would have the most relevant and positive impact on an agency's IT management capabilities, as well as its ability to deliver the IT infrastructure necessary to create a modern, 21st century digital government.

For reference, below is the summary of the latest (Version 13.0) FITARA Scorecard.



COR Biannual Scorecard - December 2021

Agency	Nov 2015	May 2016	Dec 2016	June 2017	Nov 2017	May 2018	Dec 2018	June 2019	Dec 2019	Aug 2020	Dec 2020	July 2021	Dec 2021	Agency CIO authority enhancements	Transparency and risk management	Portfolio review savings	Data center optimization initiative	Modernizing Government Technology	Cyber	Transition off Networx	CIO's boss = head or deputy	CIO Status
	1	2	3	4	5	6	7	8	9	10	11	12	13	Incremental	Dashboard	PortfolioStat	DCOI	MGT	FISMA	EIS		
USDA	D	C	C-	C-	C-	D-	D-	C-	C+	B+	B+	B+	C+	C	C	C	A	A	C	F	Y	Permanent
DOC	B	B	B+	B+	B+	C+	C+	C+	C+	B+	C+	C+	B+	A	A	A	A	B	C	F	Y	Permanent
DOD	D	D	D+	F+	F+	F+	D+	C+	C+	C+	C+	C+	C+	F	C	D	A	C		F	Y	Permanent
Ed.	F	D	C+	C+	B+	B+	B+	B+	A+	B+	B+	B+	B+	A	A	B	A	B	C	F	Y	Permanent
Energy	F	C	C-	C-	D+	C+	B+	C+	C+	C+	C+	C+	C+	A	D	C	A	C	D	F	Y	Permanent
HHS	D	D	D-	D-	D-	C-	B+	C-	C-	C-	B	B	B	B	A	A	A	C	D	C	P	Acting
DHS	C	C	B-	B-	C-	D-	C-	D-	B	C	C	C	B	B	B	B	A	B	B	F	P	Permanent
HUD	D	D	C-	B-	C-	C+	C+	C+ B+	C+	C+	C+	C+	C+	A	C	F	A	C	D	F	Y	Permanent
DOI	C	C	B+	C+	C+	C+	C+	C+	C+	C+	C+	B+	C+	B	B	C	A	B	D	F	Y	Acting
DOJ	D	C	B-	B-	C-	D-	D-	C-	C-	C-	C-	D-	C-	C	A	C	A	C	B	D	N	Permanent
DOL	D	C	C-	D-	D-	C-	B-	B-	C-	C-	B-	B-	B-	A	A	A	A	A	B	B	N	Permanent
State	D	D	D-	C-	C-	D-	C-	C-	D-	C-	C-	C	B	B	B	A	A	B	C	F	P	Permanent
DOT	D	D	F+	D+	F+	C+	C+	C+	C+	C+	C+	C+	C+	F	C	B	A	C	C	F	Y	Permanent
Treas.	D	D	C-	C-	C-	D-	D-	C-	C	B	B	B	B	C	D	B	A	B	B	A	P	Permanent
VA	C	C	B+	B+	B+	C+	B+	B+ C+	B+	C+	B+	C+	C+	A	C	D	A	D	D	C	Y	Permanent
EPA	C	C	B+	B+	C+	C+	C+	D+ C+	C+	B+	B+	B+	B+	A	B	C	A	A	D	F	Y	Permanent
GSA	B	C	B+	B+	B+	B+	B+	B+	A+	A+	B+	A+	B+	A	A	A	A	A	A	F	Y	Permanent
NASA	F	F	C+	C+	C+	C+	B+	D-	C+	C+	C+	C+	C+	F	F	A	A	B	C	F	Y	Permanent
NSF	D	D	C-	C-	C-	B+	B+	B+	B+	B+	B+	B+	A+	A	A	B	A	C	A	A	Y	Permanent
NRC	C	C	C-	C-	C-	D-	D-	C-	D-	C-	C-	C-	C-	B	B	C	A	C	B	A	N	Permanent
OPM	D	C	C+	D+	C+	D+	D+	D+	C+	C+	C+	C+	B+	A	C	A	A	B	C	F	Y	Permanent
SBA	D	D	D-	D-	C-	D+	B+	B+	B+	B+	C+	C+	C+	C	B	D	A	A	C	F	Y	Permanent
SSA	D	C	B+	C+	C+	C+	B+	B+ C+	C+	B+	C+	B+	C+	F	D	A	A	C	C	D	Y	Permanent
USAID	D	D	D-	A-	A-	C-	B-	B-	A	A	B	B	A	A	A	B	A	B	B	A	P	Permanent
													7	Project level	Tiers	Tiers	Weighted		Letters	IG & CAP	90% goal	Y-N drop
													13	DOD alt source	DOD alt source	Dashboard	30 30 20 0 20 0					
													4		PY		Scale:10					
														<=190	86631	86631					90% by Mar '22	
A				1	1				3	2		1	2	11	8	8	24	5	2	4	16 Y	22 permanent
B	2	1	8	7	4	3	11	8 7	4	8	10	10	10	5	6	6		9	6	1	3 N	2 acting
C	5	12	10	10	14	12	7	12 14	15	14	14	12	12	4	6	6		9	9	2	5 P	
D	14	10	5	5	3	8	6	4 3	2			1			3	3		1	6	2		
F	3	1	1	1	2	1								4	1	1				15		

In summary, the recommended changes to the Scorecard are:

- Evolve the current **Incremental Development** category to encompass **Modern System Development Practices** with a category measuring the use of Agile, DevSecOps, and customer experience (CX) best practices in an agency.

- Evolve the **Enhanced Transparency and Improved Risk Management (OMB's IT Dashboard)** and **Portfolio Review (PortfolioStat)** categories to the **IT Modernization Planning and Delivery** category, which will codify the need for agencies to do proper IT modernization planning and develop the execution capability to deliver on those plans.

- Evolve the **Federal Data Center Optimization Initiative (FDCOI)** category to a **Cloud Computing Adoption** category to reflect the necessity of migrating to a new, modern, interoperable IT infrastructure.

- Evolve the **Modernizing Government Technology (MGT) Act** category to an **IT Budget** category that recognizes the importance of IT activity-based cost accounting along with an agency's ability to benchmark elements of its IT infrastructure and services with other agencies and private-sector corporations.

- Evolve the existing **Cybersecurity** category by measuring an agency's cybersecurity posture, including adopting modern practices, notably implementing a zero-trust architecture.

- Keep the **Transition off GSA's expiring telecommunications contracts (EIS)** category as it is.

- Evolve the **CIO Authority** category to reflect the criticality of the CIO having insight and real authority over the total agency IT budget and the procurements related to the purchasing of IT-related products and services.

- Create a new **IT Workforce** category that measures an agency's ability to address its IT workforce challenges, including an agency having understood its workforce gaps and having the ability to recruit, develop, and retain IT staff.

The figure below is a simplified view of how the Scorecard would look with all the recommended changes.

Agency	Modern System Development Practices	IT Modernization	Cloud Adoption	IT Budget	Cyber Security	EIS	CIO Authorities	IT Workforce	Overall
Agency 1	B	B	C	B	B	C	C	C	C+
Agency 2	C	B	C	D	D	C	B	C	C
Agency 3	F	C	C	D	C	D	B	D	D+

The recommended changes to the Scorecard categories are presented in more detail below. For each category, the report first describes why the category is important, then the specific recommendations on how Congress could grade each category today, and finally how each category's grading might evolve over the next few years.

In developing the recommendations on grading a category, a primary objective was to keep it simple, so the grading mechanism could be understood by all relevant stakeholders. Further, the agency data needed to grade a category must be either available publicly or easily attainable. For the majority of the FITARA Score categories, the data (including agency plans for such things as cloud and modernization plans) should be posted to the IT Dashboard, so the data sources will shift from Congressional data calls to OMB reporting. And finally, the view was to not significantly increase the number of categories in the Scorecard.

In addition to the sections below describing the categories noted above, the report contains a section describing potential additional categories Congress should consider for inclusion in the Scorecard in the future. The report's last section provides a summary table of the recommendations, showing the evolution from the latest Scorecard (version 13.0) to the proposed new Scorecard (version 14.0).

Modern System Development Practices (Evolving Category)

Why It's Important: The use of modern system development practices, notably Agile techniques and establishing a DevSecOps delivery pipeline to move to continuous integration/continuous delivery (CI/CD), is the best practice in IT management today.

Agencies should be measured in their maturity in adopting and using such practices to deliver systems to production. But agility is not limited to software development—developing an agile culture across an agency, and using techniques such as Scaled Agile can help agencies as they work to transform and modernize their business practices through the leverage of information technology. This measure would evolve the current Incremental Development grade, which measures an agency's ability to deliver increments in six months.

Methodology for Determining an Agency's Grade: The recommendation is that the Modern System Development Practices grading schema be the following:

- **A** – The use of Agile and DevSecOps, as appropriate, for all agency systems development.
- **B** – The agency has multiple system developments underway using Agile development and DevSecOps as delivery mechanisms.
- **C** – The agency has at least one pilot in place using Agile development and DevSecOps as delivery mechanisms.
- **D** – The agency does not use Agile development and DevSecOps as delivery mechanisms. The agency has developed plans to move to the use of these best practices.
- **F** – The agency does not use Agile development and DevSecOps as delivery mechanisms. The agency has no plans to move to the use of these best practices.

Data Sources: Progress can be reported through the IT dashboard or existing reporting mechanisms. Initially, Congress should have a data call to each agency where they specifically ask for each agency's:

- IT Agile and DevSecOps plans
- Any pilots underway in Agile and DevSecOps
- If these practices are used to develop systems, evidence of demonstrated use of such practices.

Evolving the Category in the Future: A request by Congress for this information will enable the Committee to provide an overall grade for the Modern System Development Practices category with the next Scorecard. This will need to evolve to where the Federal CIO's office provides guidance and collect this data instead of the Committee.

Measuring this category could evolve as additional modern system development practices are adopted in government. For instance, customer experience (CX) co-creation and user-driven design are being used extensively in the private sector and being adopted by a number of federal

government agencies. Likewise, more organizations are turning to low-code platforms to minimize having to develop custom systems in the first place. Measures of adoption of CX techniques and implementation of low-code platforms could be considered for addition to this category in the next year or two.

Cloud Computing Adoption (Evolving Category)

Why It's Important: Organizations of all types are moving to the use of cloud computing to leverage the flexibilities of modern cloud-based infrastructure. That does not mean that all applications should be in the cloud for all workloads. Still, it is critical that agencies move to leverage cloud computing where appropriate and that they have the means to migrate applications to the cloud as they work to minimize their own data center infrastructure. The recommendation is to evolve this category from the existing Federal Data Center Optimization (DCOI) category.

Methodology for Determining an Agency's Grade: A Cloud Computing Adoption grading schema under FITARA could include two elements, each of equal importance. The elements include:

1) **Cloud Computing Adoption Planning (weight – 50%).** The following could grade an agency's cloud computing adoption plan:

    - **A** – In addition to meeting the requirements for a grade of B, the agency is working to ensure it uses best practices in its migration and hosting of applications in the cloud, such as the adoption of Cloud FinOps practices and implementation of hybrid cloud strategies.
    - **B** – The agency has developed and posted a complete plan on the IT Dashboard. This plan includes an analysis of all agency applications, identification of which ones should be moved to the cloud, what cloud services would be used to support that application (e.g., IaaS, PaaS, Saas), why the applications should be moved to the cloud, and in what order. There is an organizational structure in the agency to support the migration of applications to the cloud. There are standards and processes in place for how applications are migrated to the cloud.
    - **C** –The agency has developed and posted a plan on the IT Dashboard, but the plan lacks key elements. There is an organizational structure in the agency to support the migration of applications to the cloud.
    - **D** – The agency has developed and posted a plan on the IT Dashboard, but the plan lacks key elements. There is no organizational structure in the agency to support the migration of applications to the cloud.
    - **F** –The agency has no cloud computing adoption plan.

2) **Cloud Computing Adoption (weight – 50%).** This grade would represent the percentage of agency mission and business applications that now reside in the cloud. The grading would be as follows:
    - **A** – Above 65 percent.
    - **B** – 55 to 65 percent.
    - **C** – 45 to 55 percent.

- **D** – 35 to 45 percent.
- **F** – Below 35 percent.

Data Sources: Progress can be reported through the IT dashboard or existing reporting mechanisms. Initially, Congress should have a data call to each agency where they specifically ask for each agency's:

- Cloud computing adoption plan
- The percentage of mission and business applications running in production in the cloud.

Evolving the Category in the Future: A request by Congress for this information will enable the Committee to provide an overall grade for the Cloud Computing Adoption category with the next Scorecard. This will need to evolve to where the Federal CIO's office provides guidance and collect this data instead of the Committee. This category should evolve as new cloud operational best practices and standards emerge.

IT Modernization Planning and Delivery (Evolving Category)

Why It's Important: Federal agencies are on a continuous technology modernization journey with the need to address technical debt that has accumulated over many decades. This journey never truly ends. Current systems will continue to age, technology will continue to evolve, and innovations will constantly need to be incorporated to meet cyber posture and mission delivery needs.

Previous FITARA Scorecards focus on specific improvement aspects such as portfolio management, risk management, cyber posture, adoption of incremental development, modernizing base infrastructure, adopting shared services, and ensuring flexible funding sources and streamlined acquisition approaches are in place to support execution. These areas must have focus. Still, there needs to be an overarching focus that integrates all these elements into a unified agency IT modernization planning and delivery category. If agencies do not have such a plan, likely the elements of the Scorecard will not be balanced to achieve optimal results. In addition to a comprehensive plan, this category needs to measure how agencies deliver on their plans by assigning higher grades when agencies deliver on key acquisitions and retire challenging to maintain and insecure legacy systems (for this recommendation, a legacy system is defined as a system that has been built using technology that is challenging to support, hard to change, and prone to security issues).

Methodology for Determining an Agency's Grade: A modernization grading schema under FITARA could include elements of prioritized modernization planning and delivering on the plan. Specifically, delivering on acquisitions that replace legacy systems and decommissioning those legacy systems.

As a first step in developing a modernization plan, agencies should view their portfolio in mission segments, where each segment supports an end-to-end mission workflow. There is a compendium of legislation, PMAs, CAP goals, memoranda, and guidance that provides a framework for IT modernization. Planning, while crucial, does not guarantee that an agency can deliver on its modernization objectives. An agency must have in place the proper execution capabilities, both in terms of the talent and experience of the workforce, along with the use of best practice processes and tools. Congress could grade the agency's ability to plan and deliver on IT modernization under the following schema:

- **A** – In addition to meeting the requirements for a grade of B, the agency has, in the past twelve months, decommissioned at least one significant legacy system that was on the list to be decommissioned in the agency's modernization plan.
- **B** – In addition to meeting the requirements for a grade of C, the agency has delivered, in the past twelve months, at least one significant acquisition or a significant increment tied to mission delivery has been deployed into an operational setting.

- **C** – The agency has developed and posted a comprehensive, agency-wide plan tied to mission strategy, supported by stakeholders, prioritizes modernization efforts based on a robust analysis of the portfolio (including the analyses of legacy systems), and is reflected in the agency budget. The agency does have standards for program and project management and associated training for project personnel.
- **D** – The agency has developed and posted a plan on the IT Dashboard but the plan lacks key elements, or does not cover the entire agency, or the prioritization of projects is not based on robust analysis. The agency does have standards for program and project management and associated training for project personnel.
- **F** –The agency does not have a complete inventory of systems and no modernization plan and accompanying roadmap. The agency does not have standards for program and project management and associated training for project personnel.

Data Sources: Measures should be based on mission outcomes and not merely on cost reductions and cost avoidance. Acceptable return on investment should focus on return on mission and should be incorporated in GPRA measures that are reconstituted to reflect outcome rather than output. Progress can be reported through the IT dashboard or existing reporting mechanisms, current and planned as described above. Initially, Congress should have a data call to each agency where they specifically ask for each agency's:

- IT Modernization plan
- Description of how the plan was developed. Specifically, this response needs to address
    - How the portfolio was evaluated
    - What evaluation criteria were used to prioritize (systems no longer supported, significant improvements to the mission, cost savings)
    - A comprehensive schedule of prioritized acquisitions
- List of systems delivered into an operational environment and systems that have been retired.
- Description of the agency's standards for program and project management and evidence of associated training for project personnel.

Evolving the Category in the Future: Reporting by agencies will enable Congress to provide an overall grade to the IT Modernization Planning and Delivery category with the next Scorecard. This will need to evolve to where the Federal CIO's office provides guidance and collect these plans instead of the Committee.

Over time, the scoring for B's and A's can evolve to more than one acquisition being delivered and more than one system retired. In regard to legacy systems, the scoring can further evolve to tracking the status of remediating (upgrade or decommissioning) legacy systems that are mission critical and mission supporting, and are more than 1 version out of date ("N or N-1"). An agency should be accountable, not just the CIO but the mission or business owners, for accelerating the

replacement of bringing those systems into current state. Not only do the outdated versions pose a cyber risk, the maintenance costs and downtime risk is also greater.

Finally, it is also recommended that once this category is established and has been in place for one year, the existing Enhanced Transparency and Improved Risk Management (OMB's IT Dashboard) Portfolio Review (PortfolioStat) categories be retired, as this new category will more accurately capture the maturity of an agency's modernization efforts.

IT Budget (Evolving Category)

Why It's Important: Leveraging limited budgets that support IT is a key element of effective technology management. The current FITARA Scorecard focuses on IT budget planning and execution primarily by assessing the extent to which an agency has implemented working capital funds authorized by the MGT Act. Measuring the impact of effective IT budgeting involves additional elements, some of which can be easily implemented with available data today, and others that could be introduced over time.

Methodology for Determining an Agency's Grade: An expanded IT Budget grading schema under FITARA could include four elements, equally weighted at 25% each, as follows:

1) **Implementation of WCFs (weight – 25%).** Under the current Scorecard, the WCF element is graded as follows: An agency receives an A if it has an MGT-specific WCF with a CIO in charge of decision-making; a B if it plans to set up an MGT WCF in the current or next fiscal year; a C if it has a department WCF or equivalent; a D if it has some other IT-related funding method; and an F otherwise. The recommendation is to change this grading rubric slightly—the key is for there to be a WCF in which the CIO is in charge of IT budget and spending decision-making. It does not matter whether such a fund is MGT-specific or of another origin. The grading would change to: A if an agency has a WCF with a CIO in charge of IT budget and spending decision-making; a B if it plans to set up a WCF for IT spending in the current or next fiscal year; a C if it has a department WCF or equivalent; a D if it has some other IT-related funding method; and an F otherwise.

2) **Adoption of activity-based costing such as "Technology Business Management" (weight. – 25%).** This category should include using the Technology Business Management (TBM) taxonomy or another activity-based costing (ABC) methodology that provides transparency for technology costs by specific category and use. Through the use of ABC, agencies better capture all IT costs and align them to the agency or citizen services they enable. Agencies could be graded on their adoption of TBM or ABC, which also enables comparison of performance to other similar-sized agencies and private-sector corporations. Measuring this category could be relatively straightforward, with an agency receiving an A if the agency is using TBM (or another industry ABC benchmark) to benchmark complex IT services; a B if the agency is using TBM to benchmark basic IT commodity services; a C if an agency fully implements the TBM taxonomy; a D if an agency partially implements the TBM taxonomy; and F if there is no use of TBM.

3) **The ability of a CIO to influence spending on IT (weight – 25%).** Best practice commercial organizations give a skilled chief information officer (CIO) real authority to ensure that IT is budgeted and spent effectively. While this has been a statutory requirement since Clinger-Cohen became law in 1996, agencies have widely varied in how they

implement that authority. A Scorecard metric could involve the proportion of spending that the CIO controls, either in a budgeted account assigned to the CIO directly or real authority to approve or disapprove of agency IT spending, relative to the overall measured IT budget that the CIO tracks. This would follow an "academic" model: 90-100 percent control would get an A; 80-89 a B; 70-79 a C; 60-69 a D; and below 60 an F. Given the importance of the agency CIO having budget authority, this measure is also included in the grading of the CIO Authorities Category.

4) **The extent of CIO involvement in the procurement of technology (weight – 25%).** FITARA requires that the CIO approve, or delegate approval for, any procurement of IT from commercial providers—to ensure proper oversight of funds after Congress has authorized the funds for spending, given that the vast majority of IT spending is executed through contracts. Measurement of this criterion could follow the same rubric described above, namely 90-100 percent control would get an A; 80-89 a B; 70-79 a C; 60-69 a D; and below 60 an F. Given the importance of the agency CIO having authority over IT-related procurements, this measure is also included in the grading of the CIO Authorities Category.

Data Sources: For the near term, the agency (in particular the CIO) can report on all elements above.

Evolving the Category in the Future: As better data becomes available via TBM on how agencies spend their technology for different kinds of functions, metrics could be developed to assess technology spending as a proportion of overall program spending by agency or function. This could start by looking at the size of the IT spend relative to the overall agency budget – not a perfect metric, but stripping out large entitlement programs and other similar spending can get to something that looks like an operating budget for an agency. TBM could then break this spending ratio down in different ways, potentially by functions like service provision, law enforcement, construction, military systems, etc. This could also support measuring key factors like cybersecurity as a percentage of agency spend by category. Both could then be benchmarked against industry best practices to develop a grading scheme.

Cybersecurity (Evolving Category)

Why It's Important: Cybersecurity should always be front and center on CIO and CISO's radars. The metrics used by Congress need to address the most pressing cyber risks and use metrics aligned with Executive Order 14028," Improving the Nation's Cybersecurity."

Methodology for Determining an Agency's Grade: The current Federal Information Security Management Act (FISMA) Inspector General component of the current Scorecard becomes dated rather quickly and does not accurately characterize an agency's security posture. Specifically, Congress should phase out the Inspector General portion of the category, and metrics consistent with Executive Order 14028 and zero trust tenets (e.g., multi-factor authentication) should be used to grade agencies' cybersecurity posture. Also, Congress should consider agencies' supply chain risk management (SCRM) maturity as part of the cybersecurity grade. GAO has a comprehensive governmentwide report on SCRM that could be the basis for this grading.

The cybersecurity grade recommendation contains five elements, each weighted equally at 20% to determine a composite grade, as follows:

1) **Multi-factor Authentication (MFA) (weight – 20%).** Multi-factor authentication is a fundamental solution in identity management to reduce the risk of unauthorized access into systems. It is also a critical underpinning to zero trust. To calculate the grade, the metric is the percentage of the number of systems that use MFA in an agency out of the universe of all systems in the agency. The grading would be: more than 90 percent of systems use MFA gets the agency an A; between 80 and 89 a B; 70-79 a C; 50-69 a D; and below 50 an F.

2) **Smart Patching (weight – 20%).** How well is an agency prioritizing and applying patches across the agency to reduce the risk of software exploitation? To grade this element, an agency would answer three questions Yes/No:
    a. Does the agency have a centralized patch management process?
    b. Does the agency patching management process utilize the severity of a vulnerability to prioritize patches, e.g., CVSS?
    c. Does the agency patch prioritization process leverage automation?

    If an agency answers all three questions Yes, the agency receives an A; two Yes, the agency receives a B; one Yes, the agency receives a C; and no Yeses, the agency receives an F.

3) **Asset Management & Response (weight – 20%).** An asset management capability provides agencies with a centralized overview of their network devices and the risks associated with such devices. Asset Management identifies hardware and software located on or having access to an agency's networks. To grade this element, an agency would answer three questions Yes/No and provide one metric:

a. Does the agency have agency-wide automated hw and sw asset management and scanning tools? What percent of the agency networks and systems are covered by the tool(s)?
b. Do these tools also scan for agency-wide vulnerabilities and configuration weaknesses?
c. Are the vulnerabilities and configuration weaknesses automatically reported to the Security Operations Center (SOC) for mitigation?

If an agency answers all three questions Yes and the percent covered by the tools exceeds 80, the agency receives an A; if there are three Yeses and the percent covered by the tools is between 50 and 79, the agency receives a B; if there are three Yeses but the percent covered by the tools is less than 50, the agency receives a C; and if there are less than three Yeses, the agency receives an F.

4) **Modernizing Federal Government Cybersecurity (Zero-Trust Progress) (weight – 20%).** To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the federal government must adopt cyber security best practices, including advancing toward Zero Trust Architecture. To grade this element, an agency would answer four questions Yes/No:
   a. Does the agency have a plan to develop an agency-wide Zero Trust Architecture?
   b. Does the agency have a plan to adopt an agency-wide Zero Trust Architecture for cloud technology?
   c. Has the agency made progress toward implementing agency-wide Zero Trust Architecture? (There must be at least one ongoing project)
   d. Has the agency made progress toward implementing agency-wide Zero Trust Architecture for cloud technology? (There must be at least one ongoing project.)

   If an agency answers all four questions Yes, the agency receives an A; three Yeses, the agency receives a B; two Yeses, the agency receives a C; one Yes, the agency receives a D; and no Yeses, the agency receives an F.

5) **Foundational Practices for Managing Information & Communications Technology (ICT) Supply Chain Risks (Cyber Supply Chain Risk Management) (weight – 20%).** Federal agencies rely on information and communications technology products and services to carry out their operations. Agencies face numerous ICT supply chain risks, including threats posed by counterfeiters who may exploit vulnerabilities in the supply chain and, thus, compromise the confidentiality, integrity, or availability of an agency's systems and the information they contain. To grade this element, an agency would answer four questions Yes/No:
   a. Has the agency established executive oversight of ICT SCRM Activities?
   b. Is there an agency-wide ICT SCRM strategy?

c. Has the agency established a process to conduct agency-wide assessments of ICT supply chain risks?
d. Does the agency have an agency-wide process in operation for at least a year?

If an agency answers all four questions Yes, the agency receives an A; three Yeses, the agency receives a B; two Yeses, the agency receives a C; one Yes, the agency receives a D; and no Yeses, the agency receives an F.

During the first year of these metrics, the grades for each category should be weighted equally. In the future, the grades should be weighted to prioritize and emphasize areas with greater risk or in need of faster progress. Congress should phase out a metric when almost all of the federal government agencies have reached appropriate progress.

Data Sources: The data for these elements can come from a combination of FISMA Reporting Metrics for 2022 and DHS' Continuous Diagnostic and Mitigation Program. Other data can be reported by the agency's CIO and CISO.

Evolving the Category in the Future: The multi-factor authentication has been a requirement for the federal government since 2014. The standard practice for the government should be to purchase or develop systems that are multi-factor-authentication enabled. Hopefully, in the next few years, the metric will no longer be needed as the government will have embraced this foundational cybersecurity practice.

Some of the categories should evolve to shift from measuring the existence of plans to full program implementation. For example, Zero-Trust Progress metrics are proposed to ensure the agencies are thinking about and planning for this significant, complex modernization effort. The metrics should evolve to measure the progress toward full, agency-wide deployment of all elements of zero trust. Likewise, in cyber supply chain risk management, the measure should evolve to include an agency program that would address the elements of SCRM that are contained in NIST publication 800-161.

CIO Authorities (Evolving Category)

Why It's Important: The basis for the passage of FITARA was to ensure that an agency CIO has the authority to ensure there is appropriate IT management disciplines in place across an agency. This is the foundation for all the other FITARA Score categories. It is exceptionally difficult for an agency CIO to implement IT management best practices across an agency without the appropriate authority.

Methodology for Determining an Agency's Grade: An expanded CIO Authorities grading schema under FITARA could include three elements, equally weighted at 33%, as follows:

1) **Having the appropriate reporting structure (weight – 33%).** Under the current Scorecard, agencies are graded based on whether the CIO reports to the agency head or deputy. This measure should stay and an agency receives an A if the CIO reports to the agency head or deputy, and an F otherwise.

2) **The ability of a CIO to influence spending on IT (weight – 33%).** Best practice commercial organizations give a skilled chief information officer (CIO) real authority to ensure that IT is budgeted and spent effectively. While this has been a statutory requirement since Clinger-Cohen became law in 1996, agencies have widely varied in implementing that authority. A Scorecard metric could involve the proportion of spending that the CIO controls, either in a budgeted account assigned to the CIO directly or real authority to approve or disapprove of agency IT spending, relative to the overall measured IT budget that the CIO tracks. This would follow an "academic" model: 90-100 percent control would get an A; 80-89 a B; 70-79 a C; 60-69 a D; and below 60 an F. This measure is also used as part of the grading for the IT Budget category.

3) **The extent of CIO involvement in the procurement of technology (weight – 33%).** FITARA requires that the CIO approve, or delegate approval for any procurement of IT from commercial providers—to ensure proper oversight of funds after Congress has authorized the funds for spending, given that the vast majority of IT spending is executed through contracts. Measurement of this criterion could follow the same rubric described above, namely 90-100 percent control would get an A; 80-89 a B; 70-79 a C; 60-69 a D; and below 60 an F. This measure is also used as part of the grading for the IT Budget category.

Data Sources: Congress can ask for the agency CIO to report on the elements above.

Evolving the Category in the Future: The three elements above will effectively grade an agency CIO's authorities. There should not be a need to further evolve this category.

IT Workforce (New Category)

Why It's Important: Finding, growing, and keeping IT people has never been easy. What has changed recently is the severity and complexity of the IT staffing problem. Today the search for skilled technology professionals has risen to a fever pitch. Why? Because the volume, complexity, and business importance of IT work have grown exponentially. Because the demand for technology professionals far outstrips supply. Because traditional employment "contracts" have been shattered and highly skilled people are highly mobile. And because the U.S. economy is booming, with unusually low unemployment rates in general. It is not a surprise that the first element in the President's Management Agenda is "strengthening and empowering the Federal workforce."

Methodology for Determining an Agency's Grade: An IT Workforce grading schema under FITARA could include two elements, with graduated weighting based on the element's importance. The elements include:

1) **IT workforce retirement eligibility (weight – 60%).** Certain agencies face upcoming critical skills shortages given much of their IT staff is already retirement eligible, and they struggle to recruit and retain younger technical talent. An agency receives an A if less than 10 percent of the IT workforce is retirement eligible; a C if less than 25 percent is retirement eligible; a D if less than 40 percent retirement eligible; and an F otherwise.

2) **IT workforce strategic plan (weight – 40%).** Understanding what an IT organization should have in terms of the number of positions, and skills and abilities for each position, is critical for maturing the organization. And understanding the current gaps against that plan is imperative when recruiting. To grade this element, an agency would answer two questions Yes/No and provide one measure:
    a. Is there an IT HR strategic plan for the agency?
    b. If so, does this plan include a workforce gap analysis, and what percentage of that gap has been closed in the past year?

    If the answers to both questions are Yes and the gap has been closed by more than 20 percent, the agency receives an A; if both questions are answered Yes and the gap has been closed by more than 10 percent, the agency receives a B; if both questions are answered Yes and the gap has been closed by less than 10 percent, the agency receives a C; and if the answer to one or both of the questions is No, the agency receives an F.

Data Sources: Some of the data on agency workforce statistics is available from OPM or agency personnel data systems. Reporting by agencies for the other data elements can be used near term.

Evolving the Category in the Future: If this new category is adopted, there will most likely need to be adjustments to the grading in the future. Of particular interest would be to add an element on education and certifications. Such an element should include an effort to collect data to ensure an

agency's IT employees can effectively fill the roles of their positions. The use of individual development plans (IDPs), for instance, would show that agencies are proactively planning with their employees for their professional development. There should be consideration of adding other elements as well, including rating diversity of the IT workforce, recruiting techniques used, and the overall recruiting success rate.

Given many IT organizations have significant contractor workforces, a further evolution would involve HR planning that goes beyond the federal IT workforce in an agency. The IT workforce strategic plan measure could evolve to include the totality of the agency IT workforce, to include contract staff as well.

Potential Future Categories

In addition to the changes recommended earlier in this report, Congress should consider two categories for addition to the Scorecard in the future: customer experience (CX) and cross-agency collaboration.

CX is an essential aspect of delivering overall customer satisfaction from IT, and in recent years it has been gaining more importance across federal government agencies. In December 2021, the President issued an executive order (EO) on CX, and there is pending legislation on CX in Congress. Some models have been developed in the private sector for measuring maturity in providing CX. The recommendation above for Modern System Development Practices includes an element for CX best practices for co-creation and user-driven design. But there should be an effort to identify how mission benefits of agency CX efforts can be measured and added as a category to the Scorecard.

Secondly, there are many instances in which the provision of a product or service from an agency requires cooperation with one or more other agencies. How well a set of agencies cooperates has a significant impact on the quality and efficiency by which an agency delivers its products or services. While perhaps difficult, grading how well an agency collaborates with other agencies is a meaningful category that warrants further exploration.

The project team members preparing this report felt that while important, these two categories could not easily be graded at present. Either the measures themselves are still immature, or the required data would be difficult to gather. Further, given the recommendations for near-term changes to the Scorecard are substantial, the recommendation is to implement those first and investigate the potential addition of these two categories over the next two years.

Summary

The table below summaries the changes to the FITARA Scorecard if the recommendations in this report are adopted. The number of graded categories would increase by one to nine, and two of the categories would remain the same from version 13.0 to version 14.0 of the Scorecard.

FITARA Scorecard Version 13.0 (December, 2021)	Recommended FITARA Scorecard Version 14.0 (Summer, 2022)
Incremental Development	**Modern System Development Practices** • Update the grading approach with three key elements - Adoption of Agile - Adoption of DevSecOps - Adoption of Customer Experience (CX) practices for co-creation and user-driven design
Enhanced Transparency and Improved Risk Management (OMB's IT Dashboard) **Portfolio Review (PortfolioStat)**	**IT Modernization Planning and Delivery** • Evolving category with the following elements - Development of an agency-wide IT Modernization Plan - Delivery of elements of the IT Modernization Plan Retire the **Enhanced Transparency and Improved Risk Management (OMB's IT Dashboard)** and **Portfolio Review (PortfolioStat)** categories in one more year
Federal Data Center Optimization Initiative (DCOI)	**Cloud Computing Adoption** • Evolving category with the following elements - Cloud Computing Adoption Planning - Cloud Computing Adoption
Modernizing Government Technology Act (MGT)	**IT Budget** • Keep MGT and enhance this category with the following - Use of activity-based costing - CIO authority over IT budgets - CIO authority over IT procurements
Federal Information Security Modernization Act of 2014 (FISMA)	**Cybersecurity** • Update the grading approach with five key elements - Multifactor authentication (MFA) - Smart patching - Asset management and Response - Zero-trust progress - Cyber supply chain risk management
Transition off GSA's expiring telecommunications contracts (EIS)	**Transition off GSA's expiring telecommunications contracts (EIS)** • No change from Version 13.0
CIO Authority (CIO reporting structure)	**CIO Authorities** • Keep CIO reporting structure and enhance this category with the following - CIO authority over IT budgets - CIO authority over IT procurements
	IT Workforce • New category with the following elements - IT workforce age and retirement eligibility - IT workforce strategic plan

Summary of Recommended Changes between FITARA Scorecard 13.0 and 14.0

This project team recognizes that Congress and GAO may face challenges in evolving the Scorecard. The work required to interface with federal agencies to collect the data needed to appropriately grade each category can be significant. As a final recommendation, ACT-IAC, in its mission as serving as a trusted agent to improve government through the effective use of technology, is willing to continue to support this important work by facilitating engagement with government and industry leaders to develop best practices and lessons learned on identifying authoritative data, improving data availability, offering analytical approaches and ensuring common understanding of scorecard requirements and results.

This project team believes that if Congress implements the changes to the FITARA Scorecard recommended in this report, it will have a profound positive impact on agencies improving their ability to support their agency missions through the effective use of information technology.

Appendix - Project Team Members

The recommendations in this report represent the consensus view of 11 project team members, all of whom have significant experience in dealing with federal government information technology. The group consists of individuals with policy, management, operational, and legislative backgrounds—thus ensuring the project team considered various viewpoints when developing recommendations to evolve the FITARA Scorecard.

The project team members include:

- Jonathan Alboum, former CIO of the U.S. Department of Agriculture (USDA)
- Alan Balutis, former CIO of the U.S. Department of Commerce
- Rich Beutel, former Congressional Lead Acquisition and Procurement Policy Counsel (including being the legislative manager of FITARA)
- Dan Chenok, former Branch Chief for Information Policy and Technology with the Office of Management and Budget (OMB)
- Casey Coleman, former CIO at the General Services Administration (GSA)
- Margie Graves, former Deputy Federal CIO
- Essye Miller, former Deputy CIO at the U.S. Department of Defense (DoD)
- Dave Powner, former Director, IT Issues, at the U.S. Government Accountability Office (GAO) (supported Congress in developing the original FITARA Scorecard)
- Richard Spires, former CIO at the U.S. Department of Homeland Security (DHS)
- Dave Wennergren, former CIO at the U.S. Department of the Navy
- Renee Wynn, former CIO at the National Aeronautics and Space Administration (NASA)