U.S. House of Representatives Committee on Oversight and Reform
Subcommittee on Government Operations
January 20, 2022 Hearing
Federal Information Technology Acquisition Reform Act (FITARA) 13.0
Questions for the Record Submitted to Ms. Ann Dunkin

QUESTIONS FROM CHAIRMAN GERALD E. CONNOLLY

Q1. How might the FITARA Scorecard evolve to be a more useful tool for the Department of Energy (DOE) and Congress?

A1. Since FITARA was instituted in 2014, IT acquisition management and IT budgeting practices have evolved significantly. The most useful metrics are those that drive clearly understood outcomes, avoid unintended consequences, align with the statutory intent of FITARA, and measure progress toward implementing the Common Baseline elements identified in the Office of Management and Budget (OMB) Memorandum M-15-14: Management and Oversight of Federal Information Technology. For example, many of the current FISMA metrics that are used to build the Cybersecurity metric are pass/fail or consolidate several outcomes that result in a “fail” if not all benchmarks are achieved. These metrics should more accurately reflect the progress of departments and agencies.

The Chief Information Officer (CIO) Council has set up a working group to develop proposals for FITARA scorecard revisions. I believe consulting with the CIO Council would be the most appropriate path for the Subcommittee to obtain input from across the government for a new set of metrics.

Q2. More than half of all cybersecurity incidents occur through third-party access to IT systems. Please explain how DOE manages cybersecurity risks associated with its IT supply chain. Does DOE have a supply chain or IT vendor risk management program? If yes, please describe the program and provide the Committee with any relevant documents.

A2. DOE manages cybersecurity risks associated with its IT supply chain through a partnership between the Office of the Chief Information Officer (OCIO), the Office of Intelligence and Counterintelligence (IN), and the Office of Cybersecurity, Energy Security and Emergency Response (CESER). For federal procurement actions, the Department primarily relies on the OCIO Information, Communications and Technology (ICT) Supply Chain Risk Management (SCRM) program. This program supports risk assessments, risk treatment, and monitoring with the goal of enabling DOE leaders to make risk-informed procurement decisions, reduce the risk ICT suppliers present to the DOE, and meet regulatory requirements. The DOE SCRM program uses three types of assessments scaled to meet the risk of a particular ICT supplier. Since establishment in 2019, the SCRM program has completed more than 2,400 assessments and has been utilized by 45 different entities, including 42 DOE Departmental Elements (DEs), and three interagency partners who leverage this best-in-class program.

The DOE SCRM program utilizes four risk lenses to enable a complete picture of a supplier and the potential risks they may present to the DOE or our customer departments.

1) Cybersecurity: The Cybersecurity risk lens provides a NIST (National Institute of Standards and Technology) 800-53 (Security and Privacy Controls for Information Systems and Organizations) cybersecurity control-based evaluation of a supplier’s service and/or product.
2) Foreign Interest: The Foreign Interest risk lens assesses supplier ownership, board composition, office locations, and hiring practices to evaluate potential relationships with adversarial countries and personnel who may be on a U.S. Federal Government exclusion list.
3) Resilience: The Resilience risk lens focuses on the ability for a supplier to recover quickly from disruptions in the market and includes evaluations on financial stability, supply chain relationships, and geographic footprint.
4) Compliance: The Compliance risk lens assesses if a supplier has a historically documented regulatory finding focused on financial, antitrust/market manipulation, exports, corruption, or environmental regulatory findings.

The three types of risk assessments provided by the ICT SCRM program are:

U.S. House of Representatives Committee on Oversight and Reform
Subcommittee on Government Operations
January 20, 2022 Hearing
Federal Information Technology Acquisition Reform Act (FITARA) 13.0
Questions for the Record Submitted to Ms. Ann Dunkin

1) Prescreen assessment – Data-driven assessment to identify initial risk indicators of a supplier utilizing open source and subscription-based data.
2) Rapid assessments – Assessor-conducted analysis of a supplier's service or product while incorporating organizational impact utilizing opens source, subscription, and government-based data.
3) Deep dive assessments – Assessor-conducted analysis where security control questionnaires are sent to a supplier to validate the existence of controls within a supplier's environment.

In addition to the OCIO efforts, DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) leads the Department's Cyber Testing for Resilient Industrial Control Systems (CyTRICS) program. CyTRICS is DOE's program for cybersecurity vulnerability testing, digital subcomponent enumeration, and forensic assessment of control system technologies. CyTRICS leverages best-in-class test facilities and analytic capabilities at six DOE National Laboratories and strategic partnerships with key stakeholders including technology developers, manufacturers, asset owners and operators, and interagency partners.

Q3. How is DOE measuring the cybersecurity effectiveness of its IT investments?

A3. DOE does not have a formal process to measure the cybersecurity effectiveness of IT investments. We use our ICT SCRM program to pre-screen IT investments as part of the FITARA process but do not have metrics that would help us determine the cybersecurity effectiveness of investments. DOE is committed to partnering with key stakeholders across the Department and the interagency to better understand the effectiveness of our IT investments, which may include the development of measures and metrics.

Q4. How is DOE leveraging quantitative, data-driven risk management practices to help secure its IT infrastructure?

A4. DOE promotes quantitative, data-driven cybersecurity risk assessment methodologies and processes to drive risk-informed leadership decisions. In FY 2021, DOE developed a new Enterprise Cybersecurity Risk Management (ECRM) Strategy and Program Plan to expand Risk Register activities. This program integrates the Factor Analysis of Information Risk (FAIR) Methodology and cyber threat intelligence to form an enhanced risk quantification platform. On August 5, 2022, DOE released Risk Management Methodology Amplification Guidance to document this new approach and ensure alignment to DOE Order 205.1C, DOE Cybersecurity Program, NIST guidance, and other Federal guidance.

DOE conducts trainings for sites and laboratories on risk quantification. Additionally, DOE conducts onboarding events to train site and laboratory staff on the use of our risk quantification platform and conduct tailored risk assessments based on their priorities. DOE also develops targeted risk assessment blueprints to provide sites and national laboratories a guide for scoping risk scenarios and navigating the risk assessment process in DOE's approved risk quantification platform. Topics for the blueprints include Ransomware, High Value Asset Analysis, and Research Data Loss. These services are designed to mature risk assessment procedures and reporting, inform the enterprise risk register, and assist in prioritizing investments in system security.

DOE established a resource library and community of practice (CoP) to enable stakeholder learning and collaboration across the interagency. Additionally, DOE partners with the FAIR Institute to share lessons learned and best practices across the risk quantification space. These activities help the components of DOE make decisions based on risk severity and foster relationships and information sharing.

Q5. In May 2021, President Biden issued Executive Order 14028, "Ensuring the Nation's Cybersecurity," requiring that agencies adopt best practices for secure cloud services, zero trust architecture, and multifactor authentication and encryption. On January 26, 2022, the Office of Management and Budget (OMB) released a zero-trust architecture strategy, which set specific cybersecurity requirements and deadlines for federal agencies. What progress has DOE made in implementing the requirements of this executive order and the OMB strategy that followed?

A5. DOE has made steady progress in implementing Executive Order (EO) 14028, "Improving the Nation's Cybersecurity" and the Office of Management and Budget's (OMB) Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," requirements. The Department established a cross-Department Program Management Office (PMO) to manage the coordination of initiatives for this complex work. The PMO is prepared to initiate projects once funding is available.

DOE has met all requirements to date, including the development and submission of the following documents that describe the Department's progress and strategy to meet Cloud and Zero Trust Architecture (ZTA) objectives:

- Cloud Technology Adoption Plan,
- Zero Trust Architecture Implementation Plan,
- Zero Trust and Cloud Status Report,
- Sensitive Data Characteristics Report,
- Multifactor Authentication (MFA) Plan,
- Encryption Implementation Plans,
- MFA and Encryption 180-day Progress Report, and
- Vulnerability Disclosure Policy and Program.

The MFA Implementation Plan identifies three objectives to achieve MFA, including:

1) enforcing MFA for externally accessible Federal Information Security Modernization Act (FISMA) high and moderate systems;
2) enforcing MFA, as required, for all remaining systems based upon a documented risk-based assessment; and
3) transitioning to verifier impersonation-resistant credentials.

The Encryption Implementation Plan illustrates how DOE will facilitate adoption of encryption solutions.

DOE has made significant progress on vulnerability and hardware asset visibility, which falls under the Device pillar of the CISA ZTA Maturity Model. Enterprise level visibility of vulnerabilities has increased by 60% and hardware assets by 30% in the last 12 months, and we expect this to increase as more tools are procured and deployed across the Department. This progress is made possible through resources provided by CISA's Continuous Diagnostics and Mitigation (CDM) program. Additionally, CDM resources have enabled improved data integration into our agency dashboard that will provide an enterprise-level view of assets and vulnerabilities across the Department.

Finally, per OMB M-22-01, "Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (EDR)," DOE completed its analysis of the status of EDR capabilities and identified any gaps by the required deadline.

Q6. How should the FITARA Scorecard incorporate key tenets of this executive order, including the adoption of secure cloud services, zero trust architecture, and multifactor authentication?

A6. The FITARA Scorecard could be updated to align with the FY 2022 CIO FISMA Metrics. This realignment would ensure that FITARA and FISMA are driving the same priorities and efforts regarding cybersecurity. However, the FITARA scorecard should consider adjusting some of the FISMA metrics to ensure that departments and agencies receive credit for progress that results in increased security, rather than the current methodology where many metrics are pass/fail.

The CIO Council has set up a working group to develop proposals for revising the FITARA scorecard. I believe that consulting with the CIO Council would be the most appropriate path for the Subcommittee to obtain input from across the government for a revised set of metrics. The Department is committed to working with the CIO Council, GAO, and Congress to develop security metrics that more accurately reflect federal agency security postures.

Q7. Should the FITARA Scorecard more closely align with DOE's internal cybersecurity metrics to avoid redundancy? If so, in what way?

A7. The FITARA scorecard does not need to align to specific Department internal cybersecurity metrics. However, if FITARA relies on FISMA metrics to determine the cyber score, then FISMA metrics must be developed to reflect real organizational risk. DOE is encouraged by the new FY 2022 FISMA Guidance and Metrics and the shift to a more risk-based approach to cybersecurity, which aligns with DOE's approach of focusing on our highest priority mission areas and risks. We will continue to work closely with the CIO Council and OMB on efforts to continuously improve FISMA and ensure that the metrics that are tracked are timely and relevant.

Q8. According to data posted on IT Dashboard, DOE did not meet two of four fiscal year 2021 data center optimization goals: virtualization and metering. Please explain why DOE was unable to meet these goals. What are the Department's plans to make progress in these areas?

A8. DOE has closed several data centers that included many virtual servers that were metered. When we closed those data centers and the metered virtual servers went offline, our numbers for metering and virtualization both declined. This decline was enough for us to miss the two goals for virtualization and metering. While DOE did not meet these optimization goals, it was the result of progress toward the overall goal of closing data centers.

As the overall count of data centers continues to decrease, DOE expects the number of metered data centers to continue to drop. However, we project the number of metered data centers to remain the same for FY 2022. DOE will continue to examine data center energy efficiency and sustainability to better address the remaining metered facilities, as well as the virtual servers contained within those data centers. DOE will continue to aggressively push for closure of tiered centers where appropriate.

Q9. Government-owned-and-operated data centers can use excessive amounts of energy if not optimized for efficiency. Data center energy consumption represents 1-2% of global electricity use. Under OMB guidance, agencies are generally required to have advanced energy metering at federal data centers. Yet, according to work conducted by GAO, only 22% of federal data centers have electricity metering. DOE oversees the implementation of the Energy Act of 2020, which includes evaluating energy usage and efficiency of federal data centers. How can this Subcommittee ensure federal data centers become more sustainable?

A9. DOE's Federal Energy Management Program (FEMP) enables federal agencies to meet energy-related goals, identify affordable solutions, facilitate public-private partnerships, and provide energy leadership to the country by identifying and leveraging government best practices, which include standard metrics. We recommend that the Subcommittee refer agencies to the FEMP approach and require agencies to use the Power Usage Effectiveness (PUE) "family" metrics in their reporting.

We are committed to sustainability, including through increasing the energy efficiency of our data centers. To assist with optimization of energy use at data centers, DOE utilizes a collection of innovative Data Center Infrastructure Management (DCIM) tools, which we believe other federal agencies could also benefit from implementing. The DCIM tools include products developed by one of our national laboratories to improve the efficiency of our data centers with monitoring, alerts, and simulations. The tool identifies areas where we can improve energy efficiency, including by monitoring how much energy our infrastructure uses, measuring the power and utilization levels for servers, and providing key predictive analytics to increase efficiency. Among other important capabilities, it can be used to determine the best time to run large simulation models, helping us save on energy costs by scheduling jobs during off-peak hours. We would be happy to work with our interagency partners to support the utilization of these tools.

U.S. House of Representatives Committee on Oversight and Reform
Subcommittee on Government Operations
January 20, 2022 Hearing
Federal Information Technology Acquisition Reform Act (FITARA) 13.0
Questions for the Record Submitted to Ms. Ann Dunkin

Q10. Consolidating and optimizing data centers and moving to the cloud results in savings and more efficient and nimbler IT. What new FITARA metrics might empower and incentivize chief information officers (CIOs) to move to the cloud?

A10. The CIO Council has set up a working group to develop proposals for revising the FITARA scorecard. Consulting with the CIO Council is the most appropriate path for the Subcommittee to obtain input from across the government for a revised metrics, such as those that may empower and incentivize CIOs to move to the cloud.

Q11. The FITARA Scorecard grades agencies on their progress towards transitioning away from the General Service Administration's (GSA) outdated and soon-to-be-retired Networx telecommunications contract to GSA's Enterprise Infrastructure Solutions (EIS) program. In particular, the FITARA 13.0 Scorecard grades against GSA's goal of having 90% of telecom inventory transitioned by March 2022. DOE has an "F" in this category, meaning less than 54% of its telecom inventory is on EIS. Please explain DOE's grade in this category, along with the steps the Department will take to prioritize the transition. What steps will DOE take to ensure that the transition to EIS catalyzes improved agency operations and service and is not simply a check-the-box exercise?

A11. DOE's EIS migration was delayed by the late award of task orders for telecom services on the EIS contract. Once the task orders were awarded, DOE's team was able to rapidly begin to execute our existing transition plan. Even though contracts were not awarded until late 2021, as of March 1, 2022, DOE has moved 42.7% of services off expiring contracts. While DOE did not meet the interim goal reflected in the most recent FITARA scorecard, we expect to be fully migrated to EIS before the May 2023 expiration of the Networx contracts. DOE collaborated with GSA in October 2021 to conduct a Risk Assessment for Transition (RAFT) exercise that validated our projected transition completion date of March 2023. DOE's subsequent internal project planning, in conjunction with our EIS transition support vendor and our awarded EIS telecom vendors, has also corroborated the March 2023 target.

In addition, key personnel collaborated with GSA for a contingency planning session in January 2022 to identify additional contingency activities to address the risk of future transition delays. DOE is prepared to execute these options if needed. However, we are currently on track and believe we will not need to leverage the identified contingencies.

Q12. To rebuild trust with the public, the federal government must prioritize customer experience, and so the FITARA Scorecard should, too. What data would help build momentum for adopting customer-centric processes at DOE?

A12. Although DOE was not designated a high impact service agency, customer experience is important for both our public-facing services and those that support our internal staff. DOE is committed to improving customer experience by utilizing web-based analytic tools, surveys, and other means for measuring performance and effectiveness, and then improving our tools and processes in response to that feedback.

DOE will continue to work to raise awareness of these customer-centric processes and to drive adoption of the relevant metrics and tools through our robust governance bodies. DOE's governance framework includes the Cyber Council, chaired by Deputy Secretary Turk, and the Information Management Governance Board (IMGB), chaired by CIO Dunkin, which help us effectuate change, enable collaboration, initiate new value conversations, and accelerate modernization efforts across DOE.

The CIO Council has set up a working group to develop proposals for a revision to the FITARA scorecard. I believe that consulting with the CIO Council would be the most appropriate path for the Subcommittee to obtain input from across the government for a new revised set of metrics.

Q13. In June 2018, DOE originally requested more than $15 million and was awarded $3.7 million from the Technology Modernization Fund (TMF) for "enterprise cloud email." What is the status of the "enterprise cloud email" project?

A13. DOE completed the enterprise cloud email project to consolidate, upgrade, and migrate 26 on-premises systems to the cloud. DOE has migrated 15,951 mailboxes to the cloud. The Department is in the repayment phase of the project.

U.S. House of Representatives Committee on Oversight and Reform
Subcommittee on Government Operations
January 20, 2022 Hearing
Federal Information Technology Acquisition Reform Act (FITARA) 13.0
Questions for the Record Submitted to Ms. Ann Dunkin

Q14. Based on your experience, do you have recommendations for improving the overall TMF request and award process, including the transfer of funds post-award?

A14. Our recommendation is to continue to build on what the TMF Board has learned during this funding round and implement a process that allows for more transparency and a more agile approach that enables quicker review, approval, and disbursement of funds. We would also like to note that given the large number of requests received for this round of the TMF, the current $1 billion allocation is far less than the demand for TMF funding. I believe that the TMF process could be improved by reserving more funds for modernization, as well as reserving a portion of the funding for projects that improve security but do not yield payback.

U.S. House of Representatives Committee on Oversight and Reform
Subcommittee on Government Operations
January 20, 2022 Hearing
Federal Information Technology Acquisition Reform Act (FITARA) 13.0
Questions for the Record Submitted to Ms. Ann Dunkin

QUESTIONS FROM REPRESENTATIVE JODY HICE

Q1. As part of the Enterprise Infrastructure Solutions (EIS) Program, agencies are expected to transition their telecommunications contracts by May 2023. However, the December 2021 FITARA Scorecard notes that 11 federal agencies are not expected to meet an interim September 2022 milestone, and in fact 15 agencies failed to meet the March 2022 milestone identified in the Scorecard. The Department of Energy is one of the 15 agencies.

Q1A. Could you please explain the reason for the Department's failure to meet the transition deadline so far and what actions the Department is currently taking to meet future deadlines?

A1A. DOE's EIS migration was delayed by the late award of task orders for telecom services on the EIS contract. Once the task orders were awarded, DOE's team was able to rapidly begin to execute our existing transition plan. Even though contracts were not awarded until late in 2021, as of March 1, 2022, DOE has moved 42.7% of services off expiring contracts. While DOE did not meet the interim goal reflected in the most recent FITARA scorecard, we expect to be fully migrated to EIS before the May 2023 expiration of the Networx contracts. DOE collaborated with GSA in October 2021 to conduct a Risk Assessment for Transition (RAFT) exercise that validated our projected transition completion date of March 2023. DOE's subsequent internal project planning, in conjunction with our EIS transition support vendor and our awarded EIS telecom vendors, has also corroborated the March 2023 target.

In addition, key personnel collaborated with GSA for a contingency planning session in January 2022 to identify additional contingency activities to address the risk of future transition delays. DOE is prepared to execute these options if needed. However, we are currently track and believe we will not need to leverage the identified contingencies.

Q1B. How confident are you that the Department will meet the ultimate May 2023 deadline?

A1B. DOE is highly confident that we will meet the May 2023 deadline.

U.S. House of Representatives Committee on Oversight and Reform
Subcommittee on Government Operations
January 20, 2022 Hearing
Federal Information Technology Acquisition Reform Act (FITARA) 13.0
Questions for the Record Submitted to Ms. Ann Dunkin

Q2. Can you describe the burden placed on your agency due to the semiannual FITARA cadence? Does this frequency impact the accuracy of the picture presented to the Subcommittee of your agency's IT posture?

A2. The semiannual cadence of the FITARA Scorecard places a burden on the Department by requiring a significant amount of staff time to collect, analyze, and submit data for the scorecard. This burden impacts all DOE department elements. The frequency of FITARA metric collection, combined with other data calls issued to department elements, consumes significant resources and causes "data call fatigue." This results in lower quality data being provided to the Office of the CIO and, ultimately, Congress.

Q3. One of the FITARA metrics is based on a requirement of OMB to publicize detailed information on federal IT investments and requires agency CIOs to categorize their major IT investments by risk of failure using a set of pre-established criteria. DOE's score in this metric indicates that 10 percent of the Department's major IT investments were reported as at risk, leading to a 'D' grade that is second-lowest next to NASA's 0 percent.

Q3A. Please explain the value behind this metric, and what the 10 percent score means, particularly when as recently as December 2018, DOE scored a 93 percent in this metric?

A3A. Agencies determine their own CIO risk evaluation criteria and scoring methodologies, causing variation in measurement among agencies that can result in FITARA scores that are not comparable indicators of risk.

In December 2018, DOE used a different CIO risk evaluation scoring methodology. Risk scores were based on cost, schedule performance, and operational metrics for major IT investments only. In 2019, OMB added standard investments to the CIO risk process, substantially increasing the number of investments that required scoring. The calculation methodology was changed to scale for this change. At the same time, one IT major investment was restructured, lowering the dollar amount considered in the FITARA Scorecard calculation by about $186 million. During the past three years, the portfolio has changed in various ways, with some investments being eliminated and others added.

These changes caused changes in the dollars reported as well as the scores from December 2018 and December 2021.

We agree with the Subcommittee that the current risk assessment does not reflect the actual risk of DOE's investment portfolio and we are adjusting our methodology. The revised methodology and risk rating with be reflected in the 15th scorecard, later in 2022.

Q3B. Additionally, please explain how DOE defines a high-risk IT investment?

A3B. DOE categorizes investment risk as Low, Medium, or High risk in alignment with Federal IT Dashboard reporting required by OMB. DOE determines Low and Medium risk based on DOE's CIO risk rating methodology. DOE's risk scoring methodology uses four rating criteria:

1. IT portfolio investment risk scores,
2. Project performance,
3. Operational performance metrics, and
4. Technology Business Management (TBM) alignment.

The threshold for 'high risk' is based on OMB's risk area reporting. Risk scores range from '0' (i.e., no active risk) to '25' (i.e., very high probability with high impact). For DOE, the risk score range was 1 – 20. The list of risk is normalized to determine the cutoff or threshold for a high-risk score. In this case, the threshold for 'High Risk' is set at a '16' or the top quarter of possible risk scores within the DOE range of 1–20. This sets a high bar for investments that are considered high risk.

To update and streamline risk evaluations, DOE is changing the CIO risk evaluation methodology (for implementation after the FY 2023 President's Budget IT Portfolio Submission) by adding a new category of criteria—operational funding status—replacing the "operational performance metrics" criteria that are no longer required for OMB reporting. DOE is also removing the TBM alignment metric.

Also, as highlighted by Congressman Jody Hice and Carol Harris from GAO during the August 2020 FITARA Scorecard Hearing, there is a need for better-defined risk metrics that are consistent across the Federal Government. DOE looks forward to continued engagement with the Federal Government IT Portfolio Management community and GAO on improving consistency and quality of investment risk assessment and reporting.

Q4. The problem of legacy federal IT systems is a frequent focus of this Subcommittee. What are the Department's most critical IT modernization needs and how much progress are you making in addressing them? Would it be helpful to include in the FITARA Scorecard a metric to specifically track agencies' progress in updating or eliminating their most critical legacy systems?

A4. The most critical IT modernization needs include National Security Systems, systems that store critical data, industrial systems, and technologies needed to implement our zero trust and secure cloud strategies. In addition, there are a significant number of business systems across DOE that need modernization. DOE is making mixed progress towards modernization, limited by the availability of funding to support modernization projects. Tracking progress of application modernization through the FITARA scorecard would be helpful if it served to quantify the full backlog of systems requiring modernization and increase visibility of the barriers to modernization.