

EAC Program – Cybersecurity Operations Support Services (COSS)

Request for Information (RFI): RFQ1521800

Capabilities Statement

Due: September 20, 2021

Prepared by:



Submitted to:

Laura E. Edmondson
240-613-5825
Laura.e.edmondson@irs.gov

Submitted by:


Name of Business: Technuf LLC
Tax Identification Number: 27-5024380
DUNS: 078788966 | **CAGE Code:** 74VG8
Business Status: 8(a), MBE, DBE
Address: 40 W. Gude Drive Suite 220,
Rockville, MD 20850
Point of Contact:
Name: Faisal Quader

Telephone Number: (301) 526-7888
E-mail Address: faisal.quader@technuf.com



Table of Contents

| | |
|---|----------|
| TABLE OF CONTENTS | 1 |
| 1 OVERVIEW | 2 |
| 2 OUR EXPERIENCE IN TREASURY’S SYSTEMS..... | 2 |
| 3 TASK AREA 1 – PROGRAM AND PROJECT MANAGEMENT | 5 |
| 4 TASK AREA 2 – SECURITY ASSESSMENT AND AUTHORIZATION (SA&A) SUPPORT | 6 |
| 5 TASK AREA 3 – PENETRATION TESTING | 7 |
| 6 TASK AREA 4 – CYBERSECURITY TECHNICAL SERVICES SUPPORT | 8 |
| 7 TASK AREA 5 – CYBERSECURITY CONSULTING SUPPORT | 9 |

LIST OF FIGURES

| | |
|---|---|
| Figure 1. Integration Points for Deploying and Operating the IRS Enterprise Governance, Risk Management and Compliance Solution | 3 |
| Figure 2. Project Management Lifecycle | 5 |
| Figure 3. Identify, Protect, Detect, Respond, Recover Plan | 7 |

LIST OF TABLES

| | |
|--|---|
| Table 1. Technuf Vulnerability Management Case Study | 6 |
|--|---|

1 Overview



Founded in 2011, Technuf LLC is a Maryland-based Minority Owned, SBA 8(a)-certified Small Disadvantaged Business. We provide our customers with customized solutions with a unique structure that focus on delivering industry-leading technology services. We provide deep domain expertise in areas that cover Enterprise Solutions including IT Architecture, Cisco Systems Instant Connect (CIC) Comprising, radio and mobile networks, DevOps/DevSecOps, Database Design Development & Deployment, Data Analytics & Business Intelligence, Emerging Technologies and Digital Transformation, IT Engineering Support as well as Cybersecurity, Counterintelligence and Enterprise Security Management.

As a benchmark to assure our customer of global quality standards, Technuf holds several certifications including CMMI-Development (CMMI-DEV) Level 3, CMMI-Services (CMMI-SVC) Level 3, ISO 9001, ISO 2000-1, ISO 25010, ISO 27001, and ISO 28000.

Technuf has been supporting the IRS with its core mission of protecting U.S. citizens' PII/SBU information for the last ten years. We have been an integral member of all major cybersecurity programs and initiatives taken by the IRS to include Identity Access Management, Intrusion Detection, End-Points Detection and Remediation, Data Loss Prevention, Deep Packet Capture, Forensic Analysis and Litigation Support, Enterprise Governance, Risk Management and Compliance and Security Audit Log collection and aggregation and User Behavior Analytics. Currently, we are supporting several major initiatives including Enterprise Splunk deployment that is aggregating eleven terabytes of data daily, cloud migration to include M365 components including Exchange, OneDrive, SharePoint and Teams and deploying new security policies for the cloud Data Loss Prevention (DLP).

2 Our Experience in Treasury's Systems

During this period, we have integrated multiple Treasury systems including HR Connect for organizational and employee data, TFIMS for audit and POAM related data and ITM for employee and contractor training related data. The diagram below illustrates some of these integration points for deploying and operating the IRS Enterprise Governance, Risk Management and Compliance solution.

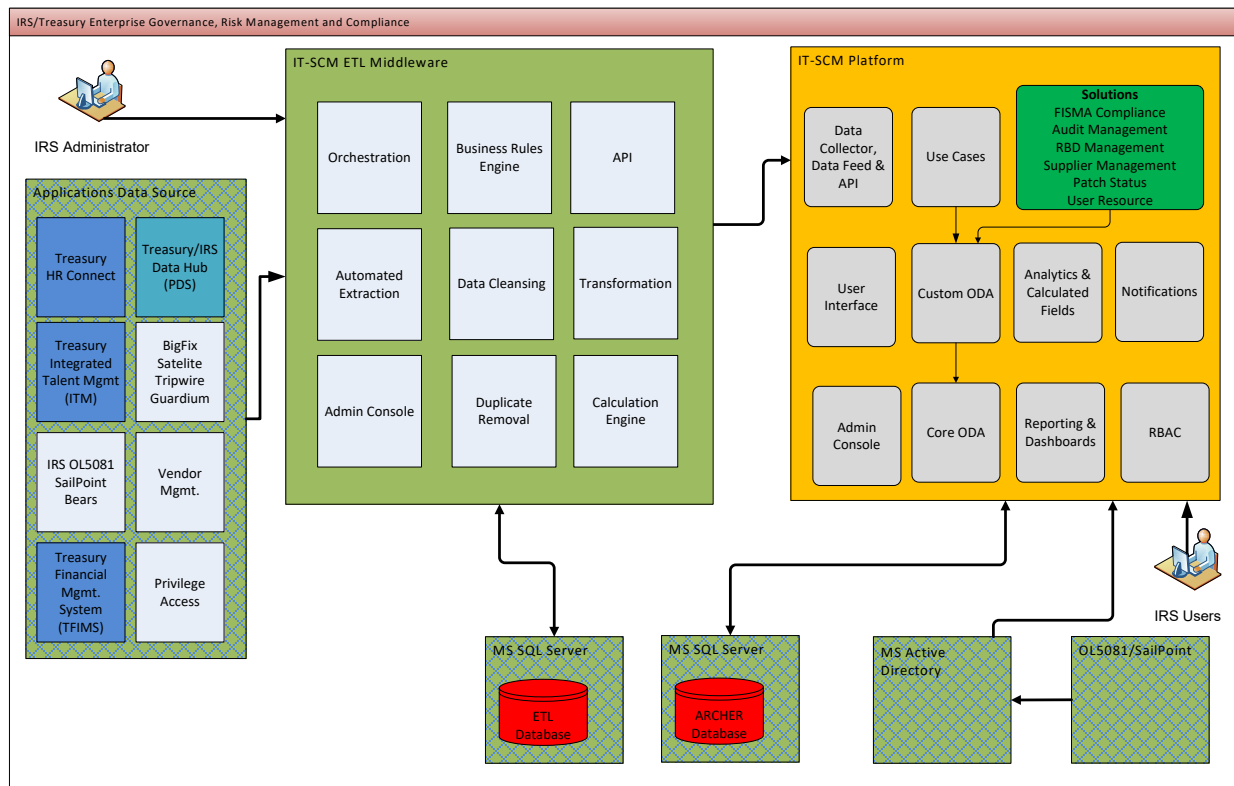


Figure 1. Integration Points for Deploying and Operating the IRS Enterprise Governance, Risk Management and Compliance Solution

Technuf led this project for a period of three years and successfully delivered multiple solutions with integrated data sets critical to the IRS functions.

1. **Audit Management** – This solution was tailored to meet Cybersecurity’s business needs for:
 - Internal compliance inspections
 - Contractor Security Reviews; and
 - Management of external audits by TIGTA and GAO. This application provides the repository for documenting audit engagements and capturing audit scope, staffing, planning, fieldwork and tracking of remediation actions. Audit Project workflows follow a comprehensive, start-to-finish approach. The application links projects to auditable entities, supports sharing of information among interdependent teams/audits, and provides ability to attach and store audit supporting documentation. The EAM Remediation sub-application is currently used by Cybersecurity and contains the JAMES audit PCAs which are tracked and reported within the Archer tool. The SRM organization within Cybersecurity oversees the Contractor Security Reviews (also known as Contractor Audit Management) and internal compliance inspections processes but is not currently using Archer to manage these processes.
2. **FISMA Training** – This solution provides the automated business process workflow for Cybersecurity, SRM, Enterprise FISMA Compliance to track and report on employee FISMA Specialized IT and DR training compliance. It enables the Business Unit Training POCs to maintain an accurate inventory of employees and contractors who are in roles requiring

specialized IT and DR training and to track their compliance. Treasury ITM is the authoritative data sources for employee training data and thus applicable data is imported into eGRC weekly to support tracking and reporting. The application can provide warning messages to individuals and then escalate to their supervisors when the FISMA training activities are not on track to complete the annual training by the scheduled completion deadline.

3. **FISMA Reporting** – System A&A and POA&M data was being imported in eGRC from Trusted Agent FISMA through June 30, 2014, until the reports were no longer available. Dashboards within this application identify compliance and non-compliance with FISMA regulatory requirements. In July 2015, TFIMS began providing the necessary system reports.
4. **Policy (EGRC-POL)** – This solution offers a centralized infrastructure for policy objectives, policy control standards and control procedures. This application also enables the mapping of policy statements to corporate objectives, federal regulatory requirements, industry guidelines and best practices. The policy information currently contained in this application is IRS IRM 10.8.1 security controls as found in NIST SP 800-53, rev 4. Control procedures, which identify how to assess the control standards, are also maintained in the application. The application also contains assessment questions to validate compliance with the NIST SP 800-53A, rev 4 controls.
5. **Incident Management** – In use by the Cybersecurity Incident and Response Center (CSIRC) since June 2012. Centralizes and streamlines the complete case management lifecycle for all cyber incidents, cyber defense measures, and other cyber policy violations, as related to unauthorized Internet browsing, etc. The capability to capture, correlate and document organizational events that may escalate into cyber incidents, evaluate incident criticality, and assign response team members based on business impact, operational responsibilities, and regulatory requirements is available. The application also allows for the consolidation of response procedures; managing the documentation and incident response procedures of all investigations from start-to-end; and reports on cyber trends, losses, recovery efforts and related cyber incidents. This solution relies heavily on the Enterprise Management solution that maintains data on personnel, organization structure, and systems and devices that comprise the IRS IT enterprise, the Threat Management solution that provides vulnerability intelligence data from security vendors and vulnerability scan data from IRS Enterprise vulnerability tools and the Policy solution that contains security controls.
6. **Vendor Management (EGRC-VNDR)** – In use by ACIO, Strategy & Planning since 2013. This solution was tailored as the Supplier Scorecard and automates and streamlines the ongoing oversight of vendor relationships. It facilitates three key activities as part of an effective vendor management process: risk-based vendor selection, relationship management, and compliance monitoring.
7. **Change Request** – This application supports management of all Archer Change Requests submitted by Solution Owners to request modifications to existing applications, reports, layout, etc.
8. **Risk Based Decision** – This application was developed to allow all IRS business units to create, track and manage risk-based decisions across the enterprise. It supports automated workflow, role-based approval cycle, automated notification and time-based triggers to ensure RBDs are approved and certified on timely basis. This solution has significantly improved the efficiency of IRS for managing RBDs. It has reduced the approval cycle from several months

to a few days to weeks. It also has provided a single automated reporting mechanisms in support of GAO and TIGTA audits.

3 Task Area 1 – Program and Project Management

We leverage our deep and broad experience across a wide range of project management methodologies and frameworks, specifically PMI / PMBOK, ITIL, Agile and Lean / Minimum Viable Product (MVP) to manage the end-to-end software design, development, and integration aspects of the overall project. Our Agile and Lean Project Management Framework offers a comprehensive set of tools and processes to address key components required to manage the end-to-end enterprise security.

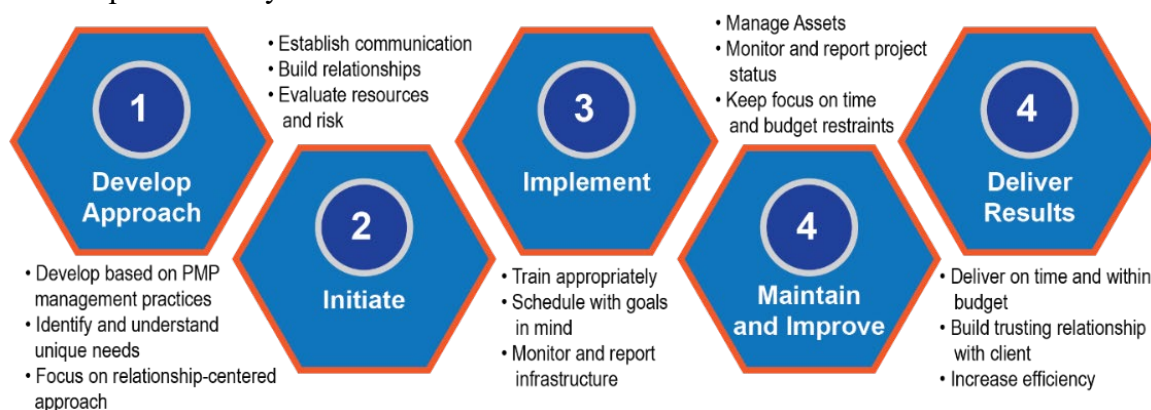


Figure 2. Project Management Lifecycle

Project and Program Management are two of Technuf’s core strengths. We leverage our Client Partner Framework (CPF), a mature and proven approach based primarily on ITIL, Project Management Body of Knowledge (PMBOK), and ISO 9001 certified approaches for project management. This provides our clients with the very best of our disciplined quality processes built around performance measures and results. We have developed this blended approach of industry best practices to optimize and serve our clients. In the table below, we list our CRF processes to provide exceptional cost control, retain quality personnel, and deliver quality services for both the short and the long term.

| CRF Process | Task Management Description |
|-------------------------------|---|
| Program Planning and Tracking | Establish policies, which emphasize coordinating and prioritizing resources across projects, departments, and entities to ensure resource contention is managed. Oversee multiple ongoing inter-dependent projects, including stakeholder management, as well as issue and risk management. |
| Risk and Issue Management | Identify and assess risks and issues. Define mitigation or corrective actions to reduce program risk and improve performance. Track risks and issues, with a defined escalation process to resolution across task orders initiatives and stakeholders. |
| Quality Management | Plan, monitor, and evaluate adherence to defined processes, procedures, and standards to achieve quality targets and identify improvements. |
| Communications Management | Identify stakeholders and the necessary communications mechanisms and flow across Technuf team, partners, and HHS. Facilitate cognizance and knowledge sharing among all stakeholders. |

| CRF Process | Task Management Description |
|------------------------|--|
| Financial Management | Manage financial resources, including accounting and financial reporting, budgeting, accounts receivable, risk management, and insurance. Assess within-budget completion, and track invoices and payments. |
| Performance Management | Develop and sustain performance-based measurement capability to support business goals including technology suitability, change impact, milestone performance, schedule, and progress. |
| Contract Management | Establish procedures for the systematic and efficient management of contract creation, execution, and analysis for the purpose of and minimizing risk and maximizing financial and operational performance. |
| Task Management | Establish and maintain project plans to provide an understanding of the tasks and track progress against schedules. Identify required staffing plans. Use Earned Value Management (EVM) to monitor and summarize performance against expectations for quality, schedule, and budget in accordance with Federal guidelines. |
| Resource Management | Establish resource plans, securing and allocating the necessary resources needed including the tracking of staff availability and related resources (e.g., technologies, facilities). Screen/select subcontractor resources. |

4 Task Area 2 – Security Assessment and Authorization (SA&A) Support

Technuf has over 10 years of experience in managing cybersecurity programs for Government and commercial customers. As part of these projects, we have worked on multiple platforms and systems and have leveraged various vulnerability management tools. One of the tools that we have deployed is Nessus. It is the industry's most widely deployed assessment solution for identifying the vulnerabilities, configuration issues, and malware that attackers use to penetrate your, or your customer's network. With the broadest coverage, the latest intelligence, rapid updates, and an easy-to-use interface, Nessus offers an effective and comprehensive vulnerability scanning package for one low cost. Our experience with Nessus has been one of the most enriching for our customers.

Table 1. Technuf Vulnerability Management Case Study

| | Description |
|---------------|--|
| Threat | <ul style="list-style-type: none"> Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features. SSL/TLS protocols use ciphers such as AES, DES, 3DES and RC4 to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that there is a stronger bias in RC4, which make statistical analysis of ciphertext more practical. The described attack is to inject a malicious JavaScript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples, that can be used for statistical analysis. |

| | Description |
|-----------------|---|
| Impact | <ul style="list-style-type: none"> If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered. This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from ciphertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie. |
| Solution | <ul style="list-style-type: none"> RC4 should not be used where possible. One reason that RC4 was still being used was BEAST and Lucky 13 attacks against CBC mode ciphers in SSL and TLS. However, TLSv 1.2 or later address these issues. |

Technuf has a proven track-record of managing security assessments tools. At the IRS we used TripWire to detect various vulnerabilities such as insecure algorithms used, SSL certificate issues, and other common exploitable vulnerabilities in order to harden the Host-based Intrusion Detection System - Endpoint Detection and Response (HIDS-EDR) servers.

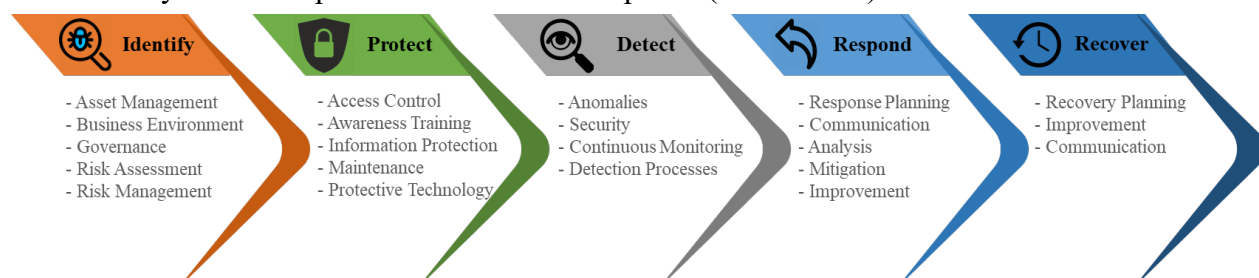


Figure 3. Identify, Protect, Detect, Respond, Recover Plan

Technuf has a proven track-record of managing security assessments tools. At the IRS we used TripWire to detect various vulnerabilities such as insecure algorithms used, SSL certificate issues, and other common exploitable vulnerabilities in order to harden the Host-based Intrusion Detection System - Endpoint Detection and Response (HIDS-EDR) servers.

Technuf uses Tenable.io™, a tool that helps solve today's toughest vulnerability management challenges. Using an advanced asset identification algorithm, Tenable.io provides the most accurate information about dynamic assets and vulnerabilities in ever-changing environments. As a cloud-delivered solution, its intuitive dashboard visualizations, comprehensive risk-based prioritization, and seamless integration with third-party solutions help security teams maximize efficiency and scale for greater productivity as listed in benefits below:

- Eliminate blind spots.
- Boost productivity.
- Prioritize cyber risks.
- Automate processes.

5 Task Area 3 – Penetration Testing

Technuf has extensive expertise providing testing services to the Internal Revenue Service (IRS). We have been part of the Enterprise Life Cycle (ELC) team at the IRS's ELC PMO office, where we implemented gates to make sure that all Information Technology (IT) projects and systems go

through a Systems Compliance Review that includes the enterprise standards by the EA group. At the end of the test cycle, we produced and submitted the End-Of-Test Completion Report (EOTCR) artifact for the stakeholders.

Vulnerability Assessment and Penetration Testing. Technuf has experience performing vulnerability assessment and penetration testing for federal agencies. Technuf delivers end-to-end penetration testing for this application. We use Nessus and CA tools to conduct vulnerability assessments.

Technuf facilitates routine penetration tests by conducting multiple simultaneous attacks across various systems to understand the feasibility of a particular set of attack vendors. We work with stakeholders to identify potential attack vectors as well as with system owners to determine what is considered in-scope for the penetration testing. To complete the process, our team will prepare a Security Assessment Report to document the results.

For the IRS's SPIIDE project, we used an enterprise risk assessment methodology where the team reviewed requirements with the SPIIDE IPT and provided feedback that allowed the IRS to prioritize requirements based on risk mitigation, ease of implementation, and user impact. The team created a risk evaluation summary detailing whether a condition is a function of a) data-in-motion (DIM); b) data-at-rest (DAR) c) data-in-use (DIU); potential impact and the likelihood of occurrence.

Technuf's Quality Assurance team brings extensive experience writing test cases from the use cases as well as conducting end-to-end testing against all applications and systems. The QA team follows strict agile methodology when conducting Quality Assurance reviews, raises bug lists, and tests results on Jira and QTP testing tools. Technuf utilizes JIRA as the case management tool for optimal case tracking systems in an Agile environment.

Test Automation. Test automation is a factor that contributed our team's success at the IRS for application deployments. We were able to reuse automation scripts for new test cases, providing efficiencies in time and cost savings. Automation also helped with regressions testing after making a new change on the software and made sure nothing breaks.

Black Box and White Box Testing. Black Box and White Box testing are strategies that adopt manual and automated script tests. Depending on the outcome of the test results, we measure and implement the appropriate remediation strategy. Technuf has hands-on experience in preparing risk-based test plans and performing security testing.

Technuf automates white box testing for efficiency. We use WinRunner to record all user activities that include opening the application login, and pressing buttons to execute certain functions within the app. Once recorded, we run the script to conduct test cases automatically. As we identify bugs, we dive into the code to pinpoint the issue on the specific module and isolate the problem. We report and open tickets with system issues via the IRS's Knowledge Incident/Problem Service Asset Management (KISAM) tool. The QA team works closely with the development team to deliver an efficient, quick solution. Our team coordinates the environment and infrastructure based on the requests and requirements gathered to support successful test execution.

6 Task Area 4 – Cybersecurity Technical Services Support

Technuf has extensive and recognized expertise in Cybersecurity. We have experience in the incident response processes as documented in the National Institutes of Science and Technology (NIST) Special Publication (SP) 800-61, Computer Security Incident Handling Guide and related DoD/DISA/NSA specific procedures.

We have supported Treasury agencies in Security Operations Center Development and the Continuity of Operation Management planning. Technuf has planned and implemented increased network security guidelines consistent with NIST, NSA, and DISA Information Condition (INFOCON) levels based on specific knowledge of various agencies and their residual Risk Assessment, COOP Plan, and historical challenges to effectively fund and exercise domain level expertise.

Technuf has extensive experience in managing IdAM (Identity and Access Management) programs. Technuf has evaluated market leading solutions that address authentication and identity proofing at multiple levels as outlined in the NIST-800-63 guideline for enterprise level deployment at large federal agencies. As part of IdAM program, Technuf has developed a consistent RBAC mechanism with approval process workflow to ensure that at all times only the appropriate individuals are given access to resources at the need-only privileges.

Technuf has developed an in-house center of excellence in Cyber security (Cyber security COE) with dedicated labs to enable our project managers and SME to architect enterprise level security and privacy frameworks that integrate current organizational initiatives with leading technologies, as well as capture organizational performance objectives that aligns technologies to the customer's strategic goals. The Cyber security COE allows the Technuf to evaluate competing technologies in a given cyber security domain, validate key assumptions, functional and performance characteristics and perform proof of concepts prior to making deployment recommendations to the end customers. The COE is continually developing and updating a combination of best of breed processes and COTS/GOTS solutions to address end-to-end cyber security requirements for the safeguard of critical private and public resources.

7 Task Area 5 – Cybersecurity Consulting Support

Technuf has been supporting the security awareness programs for several agencies, including enterprise-wide engagements with the IRS, with specialized training content and delivery in the area of Information Assurance Awareness, Personal Identifiable Information (PII), Phishing Awareness training, Personal Electronic Devices/Removable Storage Media and Sensitive but Unclassified (SBU) as well as classified data.

Technuf's expertise supported the IRS in successfully deploying the Host Based Intrusion Detection System, Endpoint Detection & Response (HIDS-EDR) solution. Technuf provided all the engineering support needed for the initial deployment, testing, and maintenance of the solution. We ensured that all business and technical requirements were met and provided all management and implementation support. Technuf provided recommendations for best practices and industry standards. IRS CSIRC did not have an effective host-based incident response capability for to speedily analyze in-depth and in real time security incidents discovered on assets in the enterprise. The HIDS-EDR solution provides the ability for CSIRC to capture inbound and outbound network traffic in real-time. It also reduces the average time to respond and conduct root cause analysis of security incidents

Before deploying the COTS FireEye HX solution in the IRS environment, we implemented it in our Center of Excellence lab to explore the potential of the solution. Technuf's deployment of HIDS/EDR results in in-depth intrusion detection and host-based forensic analysis of incidents discovered within the network. The new capabilities in the threat-response approach includes post-incident analysis, security incident investigation, Indicators of Compromise (IoC) searching, and Advanced Persistent Threat (APT) detection and mitigation. We contributed to the development

of the IoC two months ahead of schedule, setting the baseline for Release 1 and Release 2 to be executed. HIDS-EDR is a solution divided in two releases: the first deployment for workstations, and the second; deployment for servers. Release 1 included deployment to ~120,000 workstations and Release 2 included deployment to ~12,000. All milestones were met for Release 1 and we completed some milestones ahead of schedule. We performed Disaster Recovery exercises to ensure business continuity between Memphis and Martinsburg data-center locations reducing tolerable downtime from 72 hours to 6 hours after our implementation. Technuf is currently future proofing the IRS by implementing features that take a more active and blocking role within the environment rather than a detecting/passive role to boost security posture against Advanced Persistent Threats.

For the IRS RSA Archer project, Technuf developed systems that, extracted, transformed, loaded, and analyzed approximately 750,000 records with an average of 250 fields on a weekly basis. We developed a custom designed solution that gave visibility on the entire workforce training compliance against FISMA requirements. We developed an enterprise-level automated risk management solution with multi-level approvals for risk acceptance. We developed a solution to identify non-compliant and vulnerable devices across the enterprise which allowed the IRS to reduce its overall risk exposure. The implementation of the three solutions in the first bullet below allowed the IRS to be compliant with government regulations and internal policies.

Results Achieved on the IRS Archer Cybersecurity Project:

- Custom developed three complex applications over a three-year period: FISMA Security Compliance for employees and contractors, Risk Based Decision (RBD), and a Device Patch Status Solution.
- Used new business rules to develop the Device Patch Status Solution application for more than 100,000 devices.
- Developed more than 15 applications to implement new business rules, including supply management, audit management, configuration change of request, and resource management.
- Developed and designed new architecture for the entire data ingestion process to automate and optimize a mostly manual Extraction/Transformation/Load (ETL) process.
- Developed an enterprise level application for ensuring all 80,000 employees and 20,000 contractors are compliant with annual FISMA training requirements.