TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Strategies and Protocols to Authenticate Network User Identities Are Effective; However, More Action Is Needed to Verify the Identity of Devices

August 10, 2020

Reference Number: 2020-20-036

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta | 202-622-6500

Redaction Legend:
2 = Law Enforcement Techniques/Procedures and Guidelines for Law Enforcement Investigations or Prosecutions

HIGHLIGHTS: Strategies and Protocols to Authenticate Network User Identities Are Effective; However, More Action Is Needed to Verify the Identity of Devices

Final Audit Report issued on August 10, 2020
Reference Number 2020-20-036

Why TIGTA Did This Audit

The IRS manages an internal network infrastructure spanning 507 sites that allows employees, contractors, and partners to access its internal network. These users access the internal network using various devices, including desktops, laptops, wireless controllers, physical security devices, and select servers. This audit was initiated to evaluate the effectiveness of the IRS's efforts to deploy unified access controls to identify and authenticate valid user and device accesses to its internal network.

Impact on Taxpayers

IRS penetration testing disclosed significant security vulnerabilities in its internal network. These vulnerabilities indicated an unsecure internal network environment and raised the possibility of undetected accesses to sensitive information, including taxpayer data. Without properly authenticating all devices, the IRS does not have adequate controls to ensure that only authorized devices are allowed access to its internal network and taxpayer data may be at risk.

What TIGTA Found

The IRS initiated the Unified Access Project to implement a solution to correct its unrestricted internal network access vulnerability. The Cisco Identity Services Engine software product was identified as the solution to manage wired, wireless, and virtual private network access connections to the internal network.

To verify that the Identity Services Engine authentication was effective, TIGTA selected and reviewed a judgmental sample of one day of activity from the audit log. For 104,910 successful network accesses through a wired connection, 95 percent of the users and 97 percent of the devices were authenticated using certificates, and 5 percent of the users and 3 percent of the devices were authenticated using passwords. For 4,999 successful network accesses through a wireless connection, 100 percent of the users were authenticated using certificates on personal identity verification cards. However, for the devices using a wireless connection, 92 percent were not authenticated, 5 percent were authenticated with certificates, and 3 percent were authenticated with passwords. No devices connecting to the internal network through a virtual private network, *i.e.*, 26,237 successful network accesses, were authenticated.

There are approximately 91,000 Windows® compatible desktops and laptops that connect to the IRS's internal network using wired, wireless, or virtual private network connections via a secure protocol. However, there are additional devices, such as wireless controllers, physical security devices, and select servers, which are allowed to authenticate to the internal network using a less secure protocol.

Lastly, the IRS did not complete Enterprise Life Cycle methodology artifacts for the Unified Access Project, including requirements and design artifacts to aid system understanding and maintenance, as well as security, contingency planning, and testing artifacts to enable the secure operation of the Identity Services Engine.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer implement certificate-based authentication for devices wirelessly connecting or connecting through a virtual private network, coordinate with the business units to develop a comprehensive plan with milestones to reduce the number of devices that currently authenticate using a less secure protocol, and complete the Enterprise Life Cycle methodology artifacts.

The IRS agreed with all our recommendations and plans to implement certificate-based authentication for wireless devices, and dependent on funding, for virtual private network connections. The IRS also plans to develop a comprehensive plan to convert capable devices to a more secure protocol, and complete all required Enterprise Life Cycle methodology artifacts.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

August 10, 2020

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Strategies and Protocols to Authenticate Network User Identities Are Effective; However, More Action Is Needed to Verify the Identity of Devices (Audit # 201920011)

This report presents the results of our review to evaluate the effectiveness of the Internal Revenue Service's (IRS) efforts to deploy unified access controls to identify and authenticate valid user and device accesses to its internal network. This review is part of our Fiscal Year 2020 Annual Audit Plan and addresses the major management and performance challenge of *Security Over Taxpayer Data and Protection of IRS Resources*.

Management's complete response to the draft report is included as Appendix II.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Background

In Calendar Year 2012, the Internal Revenue Service (IRS) conducted penetration testing[1] that disclosed significant security vulnerabilities in its internal network, *e.g.*, local area network. These vulnerabilities included:

- Unauthorized users and devices were not prevented from connecting to the internal network and receiving unrestricted access to internal resources.
- Cybersecurity function personnel were not alerted when an unauthorized user or device attempted to connect to the internal network.

The IRS found significant security vulnerabilities in its internal network.

These vulnerabilities indicated an unsecure internal network environment and raised the possibility of undetected accesses to sensitive information, including taxpayer data. As a result, the Information Technology organization began two projects to identify and implement solutions to resolve the cybersecurity vulnerabilities. They are the Unified Access (UA) Project and the Network Segmentation Project. The goal of the UA Project is to ensure secure access regardless of connection type, *i.e.*, through wired, wireless, or virtual private network (VPN). More specifically, its purpose is to implement a solution to ensure that only valid users and devices are permitted access to the internal network. The purpose of the Network Segmentation Project is to: a) implement a solution that will allow users and devices to only navigate the network to authorized resources and b) initiate cybersecurity alerts when unauthorized users and devices attempt to connect to the internal network.

While the IRS initiated the UA Project in Fiscal Year 2012, it did not begin funding the project until Fiscal Year 2015. According to the IRS, the UA Project has spent approximately $29.4 million for hardware and maintenance, software and licenses, contractor support, *etc.*, as of May 2020. The Information Technology organization's User and Network Services (UNS) function manages the day-to-day operations of the UA Project; the Infrastructure Executive Steering Committee and the UNS Technical Infrastructure Board provide oversight and governance.

In May 2015, the UA Project team identified the Cisco Identity Services Engine (ISE) software product as its solution to correct the IRS's unrestricted internal network access vulnerability. The ISE is a security management platform that provides user and device authentication. The IRS manages an internal network infrastructure spanning 507 sites that allows employees, contractors, and partners[2] to access its internal network. These users access the internal network using various devices, including desktops, laptops, ***************2****************** wireless controllers, physical security devices,[3] and select servers.

[1] See Appendix III for a glossary of terms.

[2] According to the IRS, its partners include the Department of Homeland Security, the Government Accountability Office, the Treasury Inspector General for Tax Administration, and the Federal Emergency Management Agency.

[3] Physical security devices include badge readers, video surveillance equipment, *etc.*

Users authenticate to the internal network via the 802.1X protocol. Devices authenticate to the internal network via either the 802.1X protocol or the Media Access Control Authentication Bypass (MAB) protocol. These protocols are defined as follows:

- The Institute of Electrical and Electronics Engineers 802.1X is a standard for port-based network access control that provides an authentication mechanism for users and devices requesting internal network access. IRS users and devices use the Cisco AnyConnect software to authenticate with the ISE.
- The MAB is a method for a device that is not capable of communicating with the 802.1X protocol to be authenticated by the ISE to access the internal network. The device's media access control address is entered into the ISE on a "whitelist" so the ISE can recognize and authenticate the non-802.1X protocol compatible device.

In August 2016, the UA Project began deploying the ISE software at sites in monitor mode. Monitor mode allowed visibility into the internal network, including successful and failed authentications, but did not restrict any users or devices from accessing the network. In November 2017, the UA Project began converting sites to enforcement mode. Enforcement mode restricts users and devices from accessing the internal network until they successfully authenticate. For users, this means they must successfully authenticate using either their personal identity verification cards or use passwords generated from grid cards. For devices, this means they must successfully authenticate using either the 802.1X protocol using certificates or passwords or the MAB protocol before being granted access to the network. However, there are currently some exceptions to this requirement for devices accessing the internal network through a wireless or VPN connection.

The ISE is integrated with Microsoft® Active Directory to authenticate users and devices, *i.e.*, the ISE is added to the Active Directory domain and the ISE queries Active Directory as part of normal user and device authentication. The IRS Main Active Directory domain in the ISE for the most part refers to all IRS functions, other than Criminal Investigation. As of December 31, 2019, the IRS has enforced the authentication of users and devices for all 507 sites used by the IRS Main Active Directory domain.[4] The IRS plans to enforce authentication of the Criminal Investigation domain users and devices by December 2020.

The ISE governs three types of connections to the internal network, which are: wired, wireless, and VPN. Network access devices are the entry points for users and devices into the network. For wired connections, the network access device is an Ethernet switch. For wireless connections, the network access device is a wireless controller. For VPN connections, the network access device is an adaptive security appliance. These network access devices initiate network authentication requests to the internal network. According to the IRS, the authentication strategy is to use the following identity sources to authenticate users and devices for wired, wireless, and VPN connections.

Wired Connections:

- Users authenticate personal identity verification card certificates to Active Directory via the 802.1X protocol (approximately 75,000 users).

[4] According to the IRS, 99.9 percent of the Office of Chief Counsel domain users and devices have been migrated to the IRS Main domain as of February 12, 2020.

- Users authenticate user names and passwords to Active Directory via the 802.1X protocol (approximately 2,700 users).
- Windows®-compatible devices[5] authenticate device certificates to Active Directory via the 802.1X protocol (approximately 91,000 devices).
- Windows-compatible devices authenticate device names and passwords to Active Directory via the 802.1X protocol (approximately 91,000 devices).
- Non-802.1X protocol compatible devices authenticate using the MAB protocol (approximately ***2*** devices, including **************2****************** physical security devices, and select servers).

Wireless Connections:

- Users authenticate personal identity verification card certificates to Active Directory via the 802.1X protocol (approximately 78,000 users).
- Most Windows-compatible devices do not authenticate (approximately 60,000 devices).
- Some Windows-compatible devices authenticate device certificates to Active Directory via the 802.1X protocol (approximately 60,000 devices).
- Some Windows-compatible devices authenticate device names and passwords to Active Directory via the 802.1X protocol (approximately 60,000 devices).

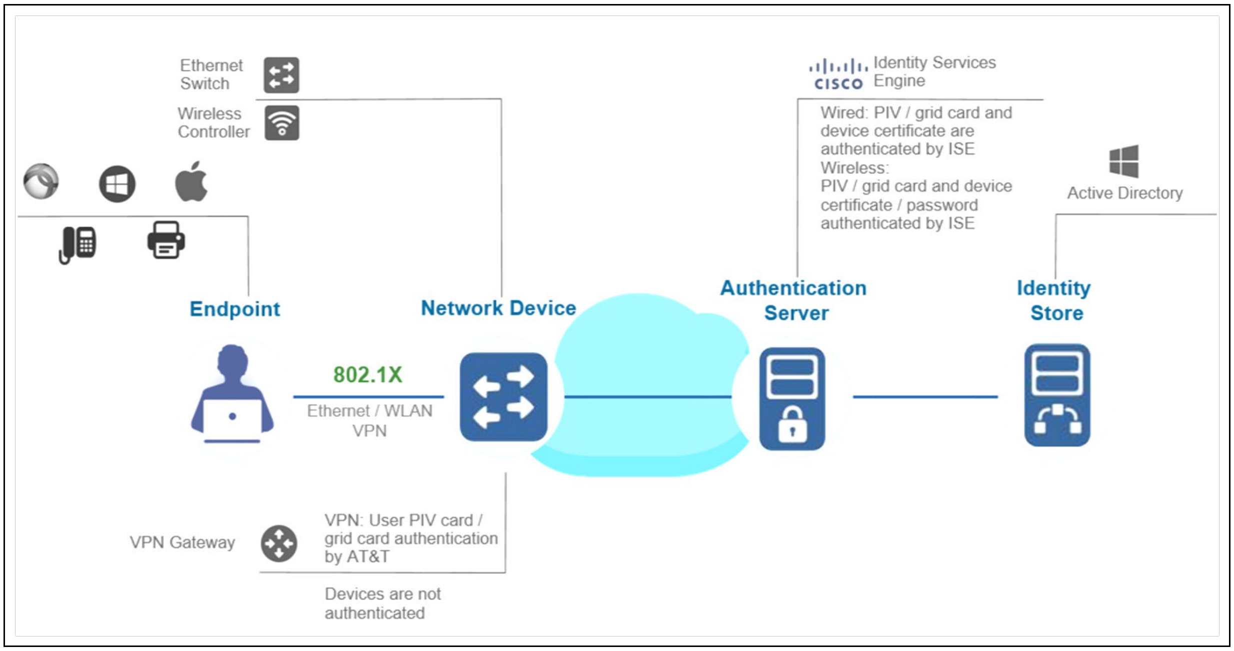
VPN Connections:

- Users authenticate personal identity verification card certificates to Active Directory via the 802.1X protocol (approximately 41,000 users).
- Users authenticate user names and passwords to Active Directory via the 802.1X protocol (approximately 700 users).
- Windows-compatible devices are not required to authenticate (approximately 60,000 devices).

For wired and wireless connections, ISE policy service nodes executing on authentication servers will make authentication decisions, either successful or failed, for users and devices requesting access to the internal network. However, for VPN connections, users working remotely use the Cisco AnyConnect software on their devices to connect through the AT&T VPN service to one of 12 Cisco adaptive security appliances. The adaptive security appliances make authentication decisions for VPN users and pass the decisions to the ISE, where the ISE blocks user accesses as needed. Figure 1 shows how authentication decisions are made for users and devices requesting access to the internal network.

[5] Windows-compatible devices are primarily desktops and laptops.

Figure 1: Authentication Decisions Made by the ISE


Ethernet Switch
Wireless Controller
Endpoint
Network Device
802.1X
Ethernet / WLAN VPN
VPN Gateway
VPN: User PIV card / grid card authentication by AT&T
Devices are not authenticated
cisco Identity Services Engine
Wired: PIV / grid card and device certificate are authenticated by ISE
Wireless:
PIV / grid card and device certificate / password authenticated by ISE
Authentication Server
Active Directory
Identity Store

Source: UA Project (as of April 28, 2020). WLAN = Wireless Local Area Network. PIV = Personal Identity Verification.

Results of Review

To verify that ISE authentication was enabled, we obtained an understanding of the authentication strategy configured in the ISE for users and devices. We reviewed evidence of identity sources defined and used, *e.g.*, Active Directory, as well as reviewed authentication policies to determine whether the authentication rules were reasonable and complete.

To verify that ISE authentication was effective, we selected and reviewed a judgmental sample[6] of one day of activity from the ISE audit log after the IRS had begun to enforce ISE authentication at all IRS sites. Figure 2 shows the summary results of our analysis of the successful user and device network accesses captured in the one day sample of ISE audit log activities.

[6] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Figure 2: Summary of Successful User and Device Network Accesses Captured in the One Day Sample of ISE Audit Log Activities[7]

	Network Connection Method		
	Wired	**Wireless**	**VPN**[8]
Successful Network Accesses	**104,910**	**4,999**	**26,237**
Users accessing the network			
Authentication by Certificate	**95%**	**100%**	**N/A**[9]
Authentication by Password	**5%**	**0%**	**N/A**
Total	**100%**	**100%**	**N/A**
Devices accessing the network			
Authentication by Certificate	**97%**	**5%**	**0%**
Authentication by Password	**3%**	**3%**	**0%**
Not Authenticated	**0%**	**92%**	**100%**
Total	**100%**	**100%**	**100%**

Source: Treasury Inspector General for Tax Administration analysis of ISE audit log activities (as of February 6, 2020).

To evaluate how the IRS managed the failed wired, wireless, and VPN authentication requests, we reviewed 30,131 rejected authentications,[10] by error type, from the sample ISE audit log activities and concluded that the reasons for the failed authentications were reasonable. According to the IRS, failed authentications are analyzed, and corrective actions are taken to resolve failed incidents. Specifically, the vast majority of failed authentication requests require remediation by Enterprise Field Operations personnel at the remote IRS sites in the form of installing or updating the Cisco AnyConnect software, correcting device certificates, or re-enabling disabled accounts in Active Directory. Further, although we did not see any suspicious devices in our review of ISE audit log activities, the IRS provided evidence that when ISE engineers identify suspicious devices, they report them to the Cybersecurity function for resolution.

[7] Authentication requests can include multiple requests from a single user or device.

[8] We did not review VPN transactions captured on the ISE audit log because AT&T authenticates VPN users. VPN transactions in the ISE audit log are actually authorization requests, not authentication requests. Authorization requests involve requesting privileges for a user, program, or process.

[9] The adaptive security appliances make authentication decisions for VPN users and pass the decisions to the ISE, where the ISE blocks user accesses as needed.

[10] There were an additional 248,713 MAB protocol authentication failures captured in the ISE audit log that we did not review. According to the IRS, network adapters initializing on Windows-compatible devices before the Windows operating system was ready to login caused these authentication failures. Because the device certificates were not initially available while the Windows-compatible devices were powering up, this forced them to attempt authentication through the MAB protocol. The ISE authentication failed due to the Windows-compatible devices not being in the whitelisted group.

Most Devices Using a Virtual Private Network or a Wireless Connection to Access the Internal Network Were Not Authenticated

Based on our review of one day of activity on the ISE audit log, we found that all devices connecting through a VPN and approximately 92 percent of devices connecting wirelessly to the internal network daily were not authenticated. This is contrary to the guidance in the Internal Revenue Manual. Internal Revenue Manual 10.8.1.4.7.2(1), *IA-3 Device Identification and Authentication*, dated July 8, 2015, states that IRS information systems shall uniquely identify and authenticate before establishing a remote or network connection.

No devices connecting to the internal network through a VPN were authenticated

The UNS function's Enterprise Remote Access Program is responsible for managing VPN access to the internal network. In the ISE architecture, ISE policy service nodes do not make authentication decisions for VPN users, as this occurs independent of the ISE software by the AT&T-managed service. Accordingly, Cisco adaptive security appliances managed by AT&T make the authentication decisions for VPN users, *i.e.*, allowing or denying VPN users access to the internal network. However, devices connecting to the internal network through the VPNs are not authenticated using either passwords or device certificates before being granted access.

Network devices connecting through a VPN to the internal network need to be authenticated.

According to UA Project personnel, in October 2019, the IRS deployed device certificates on its Windows-compatible desktops and laptops. In addition, as of February 10, 2020, the IRS substantially completed its enterprise-wide deployment of the Cisco AnyConnect (Version 4.7) on the same Windows-compatible devices. The deployment of device certificates along with the upgrade of the Cisco AnyConnect software allowed the UNS function to replace the previous device authentication protocol for wired connections, *i.e.*, replacing device names and passwords with a more secure authentication protocol using device certificates. With these changes, it is now technically possible for devices using a VPN to be authenticated using device certificates.

Enterprise Remote Access Program management explained that they currently do not have plans to enable certificate-based authentication for devices connecting through a VPN because the Cybersecurity function has not identified a lack of authentication through a VPN as a concern. However, Cybersecurity function personnel stated they have not had an opportunity to assess the risk that unauthenticated device VPN connections have on the internal network because the required Enterprise Life Cycle (ELC) methodology artifacts for security have not been completed.

Approximately 92 percent of devices connecting wirelessly to the internal network daily were not authenticated

According to the IRS, approximately 78,000 users are able to access its internal network. Of the total population of users, approximately 5,000 typically connect daily to the internal network using a wireless connection. Based on our review of one day of activity on the ISE audit log, certificate-based authentication was occurring on 5 percent of devices connecting wirelessly. Password-based authentication was occurring on 3 percent of devices connecting wirelessly. The remaining 92 percent of devices connecting wirelessly to the internal network were not authenticated. According to UNS function management, during the initial implementation of the ISE, the requirement was to implement authentication for users only.

Network devices connecting wirelessly to the internal network need to be authenticated.

According to UNS function management, certificate-based device authentication will not be fully deployed until the Cisco AnyConnect software is configured on the laptops connecting wirelessly. The UNS function plans to start configuring the Cisco AnyConnect software on the laptops connecting wirelessly in July 2020, with an expected completion date of September 2020.

Device certificates need to be fully implemented in accordance with the Internal Revenue Manual. Specifically, Internal Revenue Manual 10.8.52.4, *Certificate Usage*, dated July 5, 2019, requires the IRS to implement X.509 v3 certificates. An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure standard to verify the identity of a user, computer, or service contained within the certificate.

Because the IRS decided that the strength of the ISE authentication mechanism for wired devices is certificates, we believe that certificate-based authentication should be consistently implemented for all devices connecting wirelessly or through a VPN. Without properly authenticating all devices, the IRS does not have adequate controls to ensure that only authorized devices are allowed access to its internal network and taxpayer data may be at risk.

The Chief Information Officer should:

Recommendation 1: Require the UNS and Cybersecurity functions to coordinate with AT&T to implement certificate-based authentication for devices connecting to the internal network through a VPN.

> **Management's Response:** The IRS agreed with this recommendation. Funding dependent, the IRS will implement certificate-based authentication for devices connecting to its network via a VPN.

Recommendation 2: Ensure that the UNS function configures and implements certificate-based authentication for devices connecting wirelessly to the internal network.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will complete the work already in progress to implement certificate-based authentication for devices connecting wirelessly to its network.

************2************* Physical Security Devices, and Select Servers Used a Less Secure Authentication Protocol

There are approximately 91,000 Windows-compatible desktops and laptops that are 802.1X protocol compliant and connect to the internal network using wired, wireless, or VPN connections. However, there are approximately ***2*** additional devices, comprised of ***************2******************* physical security devices, and select servers, that are whitelisted in the ISE to allow the devices to authenticate using the MAB protocol. Figure 3 shows the type and number of devices that are whitelisted that primarily use the MAB protocol to authenticate to the internal network.

A majority of IRS devices rely on a less secure protocol to authenticate to the internal network.

Figure 3: Devices Whitelisted in the ISE

Device Type	Approximate Number of Devices
*********2**********	***2***
*********2**********	***2***
Physical Security Devices	3,000
Servers Outside Enterprise Computing Centers	1,000
Total	***2***

Source: UA Project (as of January 29, 2020).

The IRS has **********************************2** ***********2*********** that are managed internally by the IRS, and ************2************** **2**. The IRS started **********************************2** **2*************************************. This process was *************2************* the 2020 Filing Season,[11] *************2*************** *********************2************************.

All changes to the ***************************2** ********2******** to determine whether the change is *************2***************. If not, an assessment needs to be performed to determine the additional costs ********2***************** ****************2*****************. Funding has to be requested, approved, and allocated before any technical actions can occur. According to the IRS, ***************2***************** **2************.

[11] These ***2*** *2*. The IRS did this to minimize mass changes to the ISE database that might affect operational stability as well as to follow established policy that restricts making changes to critical systems during the filing season. This same policy also prevents any further mass deployment of **********2** during the filing season.

In addition, ************************************2*** **********************2******************. This is also true for the majority of physical security devices. The servers located outside of the Enterprise Computing Centers authenticate using the MAB protocol because the Cisco AnyConnect software is not compatible with servers.

Unlike the 802.1X protocol, the MAB protocol is not a strong authentication protocol because MAB authentication is vulnerable to spoofing attacks. A spoofing attack occurs when an intruder captures network traffic, intercepts the media access control addresses, and attempts to impersonate or act as one of the valid media access control addresses. Through spoofing attacks, invalid devices could access the internal network. Recognizing this vulnerability, the Draft *UA Business System Report*, dated October 2019, states that the majority of existing devices that authenticate using the MAB protocol should be converted or replaced to be 802.1X protocol compliant. While we currently believe that it is not feasible for all devices to be 802.1X protocol compliant, the IRS should make every effort to minimize the number of devices accessing its internal network that need to authenticate using the MAB protocol.

Recommendation 3: The Chief Information Officer should coordinate with the business units that internally manage non-802.1X protocol compatible devices to develop a comprehensive plan with milestones to reduce the number of whitelisted devices that currently authenticate to the ISE using the MAB protocol.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will continue to work with its business partners to develop a comprehensive plan with milestones to convert 802.1X capable devices from MAB authentication to 802.1X authentication.

Unified Access Project Management Did Not Comply With the Enterprise Life Cycle Methodology

In February 2015, the UA project manager signed a Project Tailoring Plan agreeing that the UA Project would follow the ELC methodology's commercial-off-the-shelf software development path. The commercial-off-the-shelf software development path is used when pre-packaged, vendor-supplied software will be used with little or no modification to provide all or part of the solution. The ELC methodology identifies the phases of an information technology development project, where each phase terminates at a milestone. Milestones are decision points where management reviews updated cost, progress, risk, and process information to decide if the project should continue. A Milestone Exit Review is a mandatory review conducted by the project team and Information Technology organization management when a project reaches each milestone. The outcome of the review is a go/no go decision that is documented with an unconditional approval, conditional approval, disapproval, or a recommendation to suspend or to terminate the project.

By not following the ELC methodology, critical components of the UA Project are potentially at risk.

In November 2017, when the ISE was initially deployed into production to enforce user and device authentication, the Infrastructure Executive Steering Committee had conducted and approved only the Project Initiation phase Milestone Exit Review for the UA Project. The remaining Milestone Exit Reviews were not completed for the Domain Architecture, Preliminary and Detailed Design, System Development, and System Deployment phases. The UA Project team also had not completed the required ELC methodology artifacts for requirements, design, security, contingency planning, and testing. The security artifacts that were not completed included the Systems Security Plan and the Information Systems Contingency Plan. The Information Systems Contingency Plan is important because it defines management's policies and procedures used to restore business operations, including computer operations, in the event of an emergency, system failure, or disaster.

Internal Revenue Manual 2.16.1.4.3.2, *Commercial-Off-the-Shelf (COTS) Path*, dated July 10, 2017, requires commercial-off-the-shelf projects to conduct Milestone Exit Reviews at the end of each developmental phase. The purpose of these reviews is to assess the viability of continuing the project, identifying any risks and issues, and verifying any changes to cost, scope, schedule, and business results.

In addition, the *Cybersecurity Security Change Management Standard Operating Procedure*, dated March 20, 2019, requires that information system changes are identified, managed, controlled, documented, and reviewed for impact to the security baseline of a system. Once the security change management process is initiated, the proposed changes to the system will be evaluated by stakeholders to determine the impact to the security baseline. The level of assessment determination is based on a numerical scale that indicates the necessary security activities that an information system must undergo as a result of a change. For example, a level of assessment 1 determination indicates that ELC methodology security artifacts must be updated.

The authorization to deploy the ISE into the production environment as an initial operation capability applied only to monitor (read only) mode

The UA project manager explained that a June 2016 memorandum issued by UNS function management gave the UA Project the authority to deploy the ISE into the production environment in monitor (read only) mode. The memorandum explained that a production initial operation capability would be permitted prior to completion of the ELC process; however, the UA Project team would need to complete all necessary ELC methodology requirements and milestones prior to full deployment of a UA-Network Segmentation[12] solution. When UNS function management allowed the UA Project to deploy in monitor mode in June 2016 prior to completion of all ELC requirements, they accepted the unknown security risks. According to the memorandum, this authorization was to end when the project transitioned to enforcement mode[13] or by December 31, 2017. Therefore, as of December 31, 2017, the UA Project team should have complied with the ELC methodology, *i.e.*, completed the required ELC methodology artifacts and held Milestone Exit reviews.

The UA Project needs to implement an approved security change to an existing system

According to Cybersecurity function policy, if the ISE is considered a new system, the project team is required to obtain an Authorization to Operate prior to deployment into production. Otherwise, the ISE would be considered a security change to an existing system, and the project

[12] This refers to the closely related Network Segmentation Project. For ELC methodology compliance purposes, the UA Project and the Network Segmentation Project were initially managed together; however, as of August 2017, these efforts were separated into two separate projects.

[13] Enforcement mode was initiated in November 2017 and completed in December 2019.

team would be required to follow the Change Management process. In October 2017, the Cybersecurity function completed a Control Impact Assessment for the ISE. Subsequently, the Cybersecurity Change Advisory Board reviewed the Control Impact Assessment and determined that Security Change 2017-08-2473 deploying the ISE into production in enforcement mode necessitated a level of assessment 1. A level of assessment 1 would require the UA Project team to add the ISE to an existing system's security boundary, System Security Plan, and Information Systems Contingency Plan.

In January 2020, the UA project manager explained that it is management's intention to add the ISE to the General Support System (GSS)-34 Enterprise Network security boundary. The Enterprise Network provides intranet connectivity among the various computing centers and campuses and is considered a critical infrastructure protection asset that represents a component of the national infrastructure, critical to national and economic security.

To confirm the relationship between the ISE and the GSS-34, we reviewed a March 2015 Security Change Request that identified that the ISE affected the GSS-34. Subsequently, we verified that the GSS-34's system boundary had not been revised to include the ISE, as well as the GSS-34's System Security Plan and Information Systems Contingency Plan had not been updated to include the ISE. As of April 2020, at the end of our audit fieldwork, these conditions still existed. Therefore, the UA Project team and the Cybersecurity function did not complete the necessary tasks to accomplish an approved security change to add the ISE to the GSS-34. By not following the ELC methodology, the software development, security, and contingency planning of the UA Project, as a component of a critical infrastructure protection asset, are potentially at risk.

Management Action: UNS function management notified us in March 2020 that they are in the process of updating all ELC methodology artifacts including the security boundary, the System Security Plan, and the Information Systems Contingency Plan for the GSS-34 as a result of the ISE implementation.

Recommendation 4: The Chief Information Officer should ensure that ELC methodology artifacts for the UA Project are completed, including requirements and design artifacts to aid system understanding and maintenance, as well as security, contingency planning, and testing artifacts to enable the secure operation of the ISE.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will continue work to complete all required ELC methodology artifacts.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the effectiveness of the IRS's efforts to deploy unified access controls to identify and authenticate valid user and device accesses to its internal network. To accomplish our objective, we:

- Evaluated UA Project compliance with the ELC methodology's commercial-off-the-shelf software development path.
- Verified that unified access authentication was enabled and effective for users and devices permitted access to the internal network. We obtained and reviewed a judgmental sample[1] of one day of activity from the ISE audit log for February 6, 2020.

Performance of This Review

This review was performed with information obtained from the Information Technology organization's UNS function located in New Carrollton, Maryland, during the period August 2019 through May 2020. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Bryce Kisler, Director; Carol Taylor, Audit Manager; Denis Danilin, Lead Auditor; Lauren Ferraro, Auditor; and Allen Henry, Auditor.

Validity and Reliability of Data From Computer-Based Systems

We performed tests to assess the reliability of the data from the ISE audit log file. We evaluated the data by: 1) visually reviewing the output file to detect obvious errors and unexpected missing data, 2) verifying the number of observations in the raw input file and output file are the same to ensure the completeness of the output file, and 3) communicating with IRS officials knowledgeable about the data to obtain a count of the total number of log records. We determined that the data were sufficiently reliable for purposes of this report.

Internal Controls Methodology

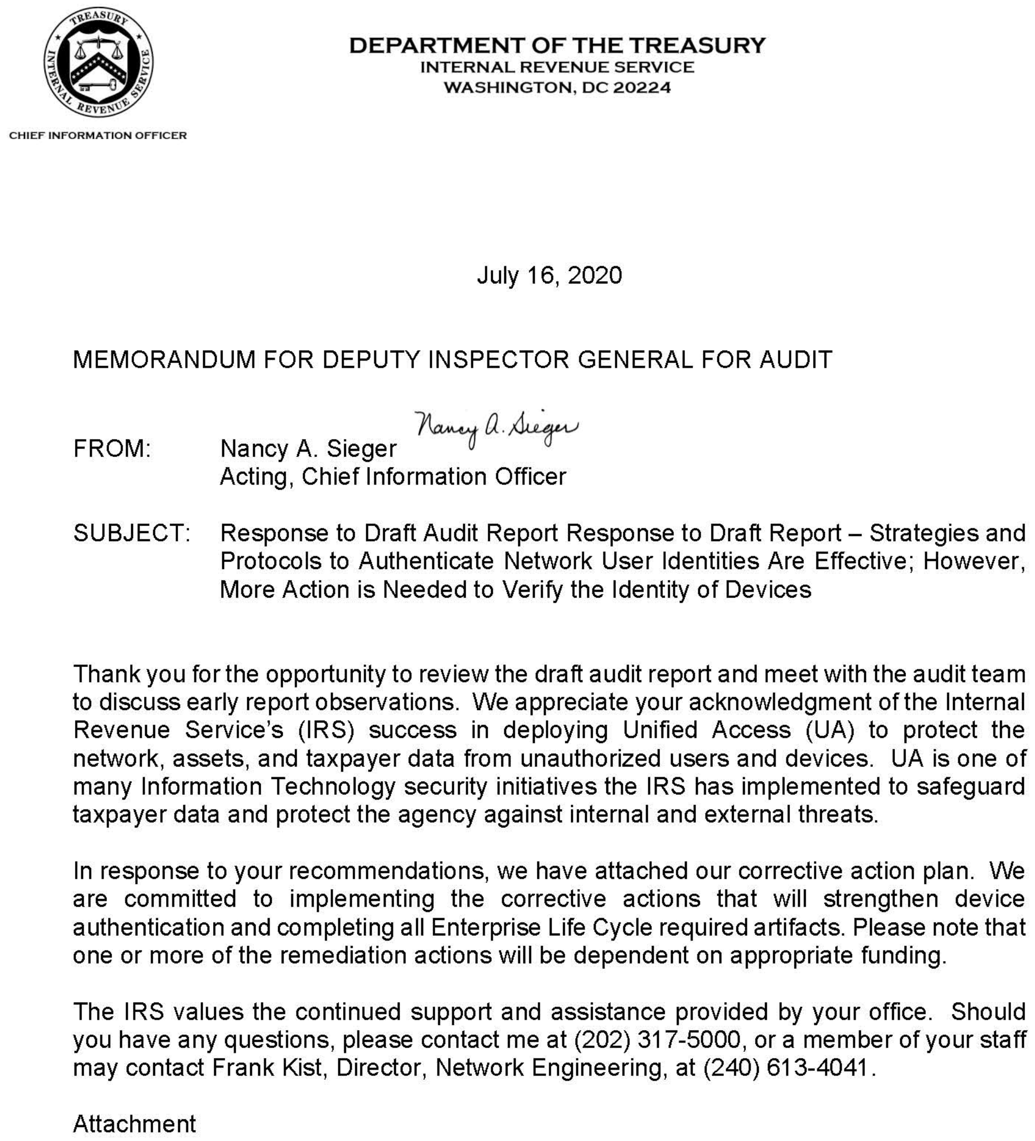
Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: IRS ELC methodology; security guidance; and ISE configuration, policies, rules, and audit logs. We evaluated these controls by

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

reviewing the criteria applicable to network authentication of users and devices, assessing the UA Project's governance process, interviewing UNS and Cybersecurity function personnel as well as reviewing and analyzing UA Project documentation. We also verified that unified access authentication was enabled and effective by reviewing and analyzing ISE configuration, ISE authentication policies and related ISE rules, and ISE identity sources. We also evaluated ISE audit log activities for February 6, 2020, to determine how the IRS manages successful and failed authentication requests.

Appendix II

Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF INFORMATION OFFICER

July 16, 2020

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger Nancy A. Sieger
Acting, Chief Information Officer

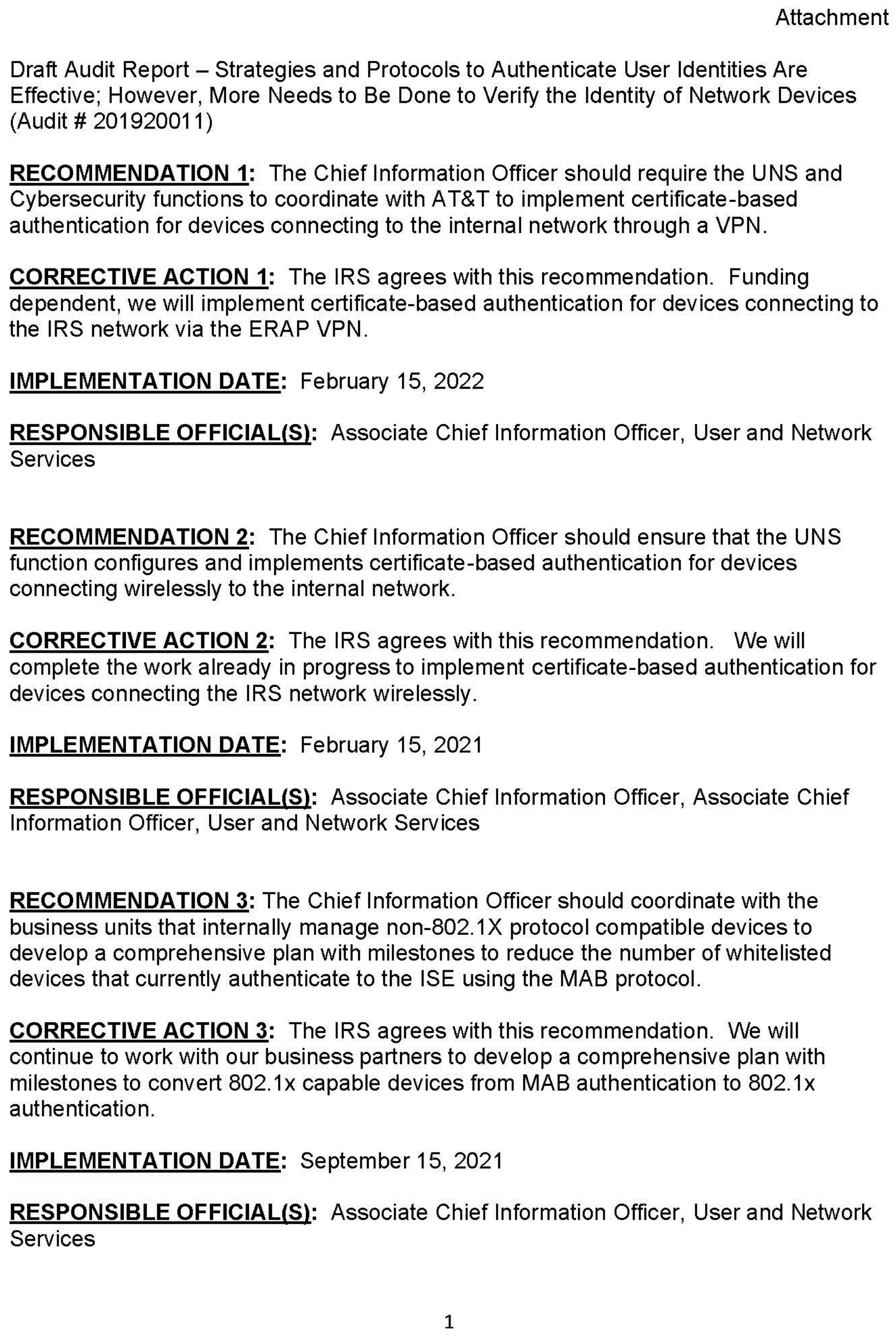
SUBJECT: Response to Draft Audit Report Response to Draft Report – Strategies and Protocols to Authenticate Network User Identities Are Effective; However, More Action is Needed to Verify the Identity of Devices

Thank you for the opportunity to review the draft audit report and meet with the audit team to discuss early report observations. We appreciate your acknowledgment of the Internal Revenue Service's (IRS) success in deploying Unified Access (UA) to protect the network, assets, and taxpayer data from unauthorized users and devices. UA is one of many Information Technology security initiatives the IRS has implemented to safeguard taxpayer data and protect the agency against internal and external threats.

In response to your recommendations, we have attached our corrective action plan. We are committed to implementing the corrective actions that will strengthen device authentication and completing all Enterprise Life Cycle required artifacts. Please note that one or more of the remediation actions will be dependent on appropriate funding.

The IRS values the continued support and assistance provided by your office. Should you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Frank Kist, Director, Network Engineering, at (240) 613-4041.

Attachment



Attachment

Draft Audit Report – Strategies and Protocols to Authenticate User Identities Are Effective; However, More Needs to Be Done to Verify the Identity of Network Devices (Audit # 201920011)

RECOMMENDATION 1: The Chief Information Officer should require the UNS and Cybersecurity functions to coordinate with AT&T to implement certificate-based authentication for devices connecting to the internal network through a VPN.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. Funding dependent, we will implement certificate-based authentication for devices connecting to the IRS network via the ERAP VPN.

IMPLEMENTATION DATE: February 15, 2022

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

RECOMMENDATION 2: The Chief Information Officer should ensure that the UNS function configures and implements certificate-based authentication for devices connecting wirelessly to the internal network.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. We will complete the work already in progress to implement certificate-based authentication for devices connecting the IRS network wirelessly.

IMPLEMENTATION DATE: February 15, 2021

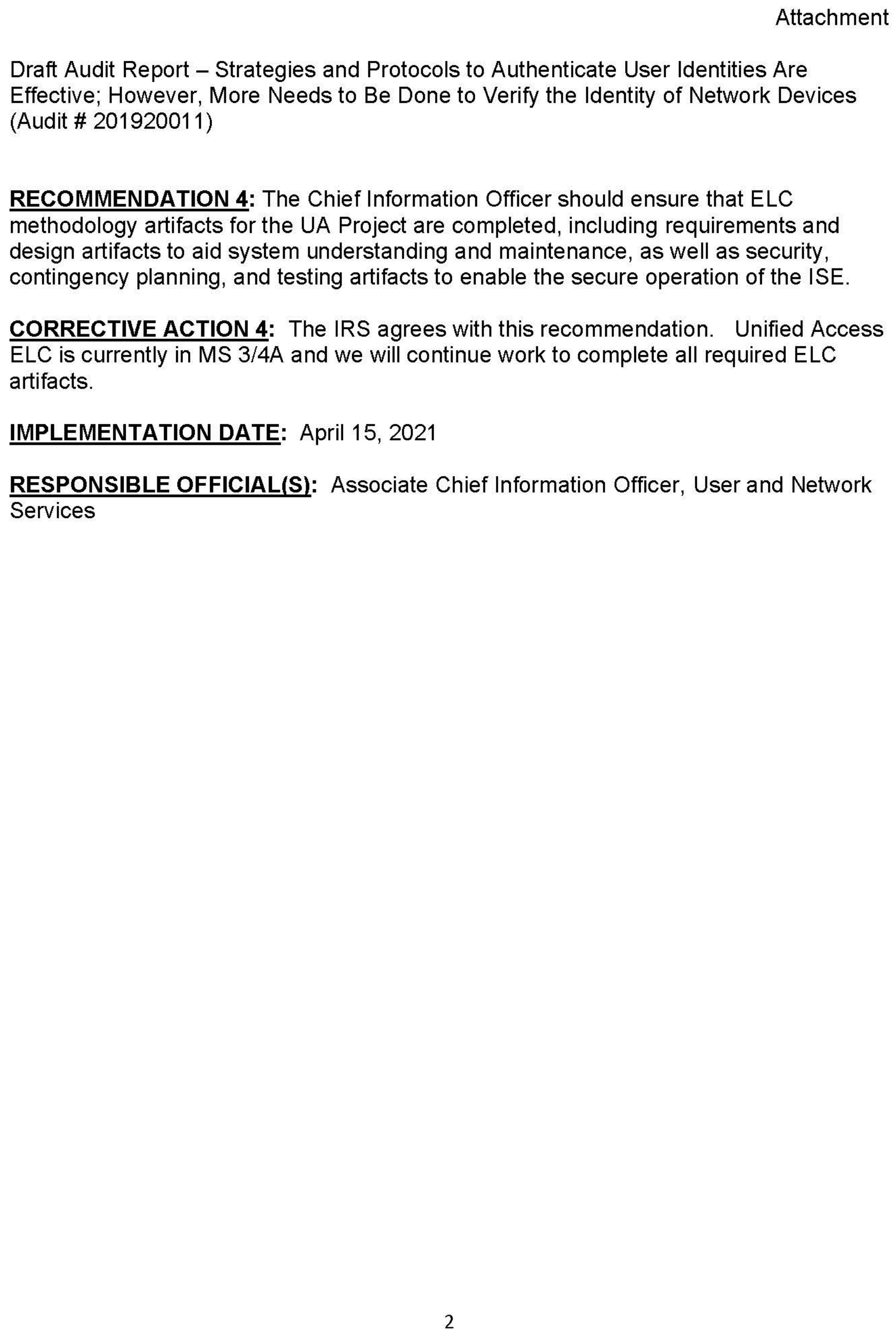
RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Associate Chief Information Officer, User and Network Services

RECOMMENDATION 3: The Chief Information Officer should coordinate with the business units that internally manage non-802.1X protocol compatible devices to develop a comprehensive plan with milestones to reduce the number of whitelisted devices that currently authenticate to the ISE using the MAB protocol.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. We will continue to work with our business partners to develop a comprehensive plan with milestones to convert 802.1x capable devices from MAB authentication to 802.1x authentication.

IMPLEMENTATION DATE: September 15, 2021

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services



Attachment

Draft Audit Report – Strategies and Protocols to Authenticate User Identities Are Effective; However, More Needs to Be Done to Verify the Identity of Network Devices (Audit # 201920011)

RECOMMENDATION 4: The Chief Information Officer should ensure that ELC methodology artifacts for the UA Project are completed, including requirements and design artifacts to aid system understanding and maintenance, as well as security, contingency planning, and testing artifacts to enable the secure operation of the ISE.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. Unified Access ELC is currently in MS 3/4A and we will continue work to complete all required ELC artifacts.

IMPLEMENTATION DATE: April 15, 2021

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

Appendix III

Glossary of Terms

Term	Definition
Active Directory	Microsoft software product that provides administrators with the means for assigning network-wide policies, deploying programs to many computer systems concurrently, and applying critical updates to an entire organization. It stores information and settings related to an organization in a centralized and accessible database.
Adaptive Security Appliance	A security device that combines firewall and VPN capabilities.
AnyConnect	Cisco software product that is a security agent (software) on a device that delivers multiple security services to protect the enterprise, including features that allow administrators to control which network or resources to which devices can connect.
Artifact	The tangible result or output of an activity or task performed by a project during its life cycle.
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Authentication	The process of verifying the identity of a user or device.
Authentication Server	An application that facilitates authentication of an entity that attempts to access a network. An authentication server can reside in a dedicated computer, an Ethernet switch, an access point, or a network access server.
Authorization to Operate	The official management decision to authorize the operation of an information system and to explicitly accept the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Change Management Process	The process responsible for controlling the life cycle of all changes, enabling beneficial changes to be made with minimum disruption to information technology services.
Control Impact Assessment	An assessment of affected security controls.
Detailed Design Phase	Involves the development of an application’s physical design and relates to how data are entered into a system, verified, processed, and displayed as output.
Device Certificate	An electronic document that is embedded into a hardware device with the certificate's purpose being to provide proof of the device's identity.
Domain Architecture Phase	Involves the development of a business system concept, business system requirements, and business system architecture.

Term	Definition
Enterprise Computing Center	A data center that supports tax processing and information management through a data processing and telecommunications infrastructure.
Enterprise Remote Access Program	The IRS's VPN solution for remote network access. The Enterprise Remote Access Program allows users to work on the IRS network, just as if they were located in an IRS facility.
Ethernet	An array of network technologies used in local area networks, where computers are connected within a primary physical space.
Ethernet Switch	A computer networking device used to connect various Ethernet devices together by using packet switching to receive, process, and forward data from one source device to another destination device.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
General Support System	Resources that provide information technology infrastructure support to applications and business functions.
Grid Card	A method of identifying users in which the user is asked to input a series of characters based on a preregistered pattern on a grid (that the user knows) and a grid of pseudo-random characters generated by the authenticator. This method results in a different series of characters each time the user authenticates.
Identity Source	A database such as Active Directory that the Cisco ISE uses to obtain user information for authentication.
Identity Store	A system that maintains identity information, *e.g.*, Active Directory. An identity store is often an authoritative source for some of the information it contains.
Initial Operation Capability	A pilot or limited production deployment used to assess its implementation to see if changes are needed prior to full production deployment.
***********2**********	************************************2*************************************** ******************2*****************.
Local Area Network	A communications network that is typically confined to a building or location.
Managed Service	The practice of outsourcing day-to-day management responsibilities and functions as a strategic method for improving operations and cutting expenses.
Media Access Control Address	A hardware identification number that uniquely identifies each device on a network.
Penetration Testing	A test methodology in which assessors, using all available documentation, *e.g.*, system design, source code, manuals, and working under specific constraints, attempt to circumvent the security features of an information system.

Term	Definition
Personal Identity Verification Cards	A U.S. Government smart card that contains the necessary data for the cardholder to be granted access to Federal facilities and information systems.
Physical Security Device	Electronic devices that include badge readers, video surveillance equipment, *etc*.
Policy Service Node	A Cisco ISE node with the policy service persona that evaluates authentication policies and makes all authentication decisions.
Port	The entry or exit point from a computer for connecting communications or peripheral devices.
Preliminary Design Phase	Involves developing the application's logical design. Logical design pertains to an abstract representation of the data flow, inputs, and outputs of the system.
Project Initiation Phase	Involves defining project scope, forming the project teams, and beginning many of the ELC artifacts.
Project Tailoring Plan	Adapts the ELC methodology to the unique and specific needs of the individual project or release. Tailoring includes selection and modification of the following ELC components to be commensurate with the scope and risk of the project: project life cycle, life cycle paths, major types of activities, work products/deliverables, data item descriptions, customer technical reviews, life cycle status reviews, and scope of management.
Protocol	A set of rules, *i.e.*, formats and procedures, to implement and control some type of association, *e.g.*, communication, between systems.
Public Key Infrastructure	An encryption system of digital certificates and other authorities that verify and authenticate the validity of each party involved in an electronic transaction.
Server	A computer or device on a network that manages network resources.
System Deployment Phase	Involves expanding the availability of the solution to all target environments and users. It results in transferring support to an organization other than the developers and signifies the end of project development.
System Development Phase	Involves coding, integrating, and testing the application. It results in the authorization to put the solution into production.
System Security Plan	A formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned.
Virtual Private Network	A secure way of connecting to a private local area network at a remote location, using the Internet or any unsecure public network to transport the network data packets privately, using encryption.
Virtual Private Network Gateway	A connection point that connects two local area networks into an unsecure network, such as the Internet.
Whitelist	If the item is on the "whitelist," then it is allowed access or execution rights in a system or network. If it is not on the "whitelist," then it is denied access or execution rights in a system or network.

Term	Definition
Windows-Compatible Device	Computers such as desktops and laptops that have the Windows operating system installed.
Wired	Utilizes physical cables and circuits contained within a specific location to access a network.
Wireless	Connects to a local area network or wireless local area network without physically connecting the device through a wired Ethernet connection.
Wireless Controller	A device that manages wireless network access points that allow wireless devices to connect to the network.

Appendix IV

Abbreviations

ELC	Enterprise Life Cycle
GSS	General Support System
IRS	Internal Revenue Service
ISE	Identity Services Engine
MAB	Media Access Control Authentication Bypass
UA	Unified Access
UNS	User and Network Services
VPN	Virtual Private Network