COMPANY LOGO HERE

CMMC Level 1 Readiness Assessment

DIB VIP Class

Cohort 1 & 2

Spring 2026

GaMEP
Georgia Manufacturing Extension Partnership

Table of Contents

SECTION I – ASSESSMENT INFORMATION

SECTION II – APPENDICES

This Cybersecurity Assessment is intended to be used exclusively by [Company Name Here]. Unauthorized disclosure or use of this information is strictly prohibited. If you have received this document in error, please permanently dispose or destroy this assessment and notify Cassia Baker immediately by sending an email to [redacted]

SECTION I – ASSESSMENT INFORMATION

1. Dates of Assessment

March 16, 2026

2. Purpose

The purpose of the project is to:

a) Perform a rapid CMMC Level 1 cybersecurity gap assessment,
b) Determine the current level of CMMC Level 1 compliance and overall basic cyber hygiene
c) Provide feedback and resources ACME Consulting can access on their journey towards CMMC Level 1 compliance
d) Offer support organization resources

3. Assessment Scope and Network Boundary

The scope of this assessment is [redacted] with a physical presence in Georgia at:

[redacted]

4. Assessment Participants

- [redacted] Owner and CEO, ej@manuafacturing.com
- Cassia Baker – Project Manager - Cybersecurity, GAMEP, [redacted]
- Michael Barker – Principal Project Manager – Cybersecurity, GAMEP, [redacted]
- [redacted] Lead Assessor – DIB Compliance VIP, [redacted]
- [redacted] Assistant Lead Assessor – DIB Compliance VIP
- [redacted] – Assessor – DIB Compliance VIP, [redacted]
- [redacted] Assessor – DIB Compliance VIP, [redacted]
- [redacted] Assessor – DIB Compliance VIP, [redacted]
- [redacted] – Assessor – DIB Compliance VIP, [redacted]
- [redacted] - Assessor – DIB Compliance VIP, [redacted]
- [redacted] – Assessor – DIB Compliance VIP, [redacted]
- [redacted] Assessor – DIB Compliance VIP, [redacted]
- Camilo Castrillon – Assessor – DIB Compliance VIP, [redacted]
- [redacted] – Assessor – DIB Compliance VIP, [redacted]
- [redacted] – Assessor – DIB Compliance VIP, [redacted]
- [redacted] – Assessor – DIB Compliance VIP, [redacted]

5. Company Background

ACME Consulting is a small business with fewer than 10 employees that provides staffing services, primarily supporting U.S. Department of Veterans Affairs (VA) hospitals by recruiting and placing medical and administrative personnel. The company operates across multiple states and functions as an intermediary, connecting qualified candidates with healthcare facilities for employment opportunities. GPI maintains relationships with third-party service providers for IT support and background check processing, introducing external dependencies into its operational environment. The organization operates under a fully remote, work-from-home model and permits the use of employee-owned devices (BYOD), which increases the complexity of securing its information systems. The company handles Controlled Unclassified Information (CUI), including personally identifiable information (PII) of candidates and staff, job requisition details, and related healthcare staffing data. Given its role, distributed workforce, and reliance on third-party services, GPI's environment presents unique cybersecurity considerations relevant to CMMC compliance and audit readiness.

6. CMMC Compliance Gap Assessment Justification

While ACME Consulting has/has not performed work as a Department of Defense (DoD) contractor, it has worked on contracts with the Georgia Department of Transportation. ACME Consulting desires to improve their basic cyber hygiene as well as become a DoD 'supplier of choice' by demonstrating it meets DoD CMMC 2.0 Level 1 cybersecurity requirements.

It is pragmatic for ACME Consulting to begin the process of CMMC compliance now and not later. The reasons include:

1. CMMC compliance is not easy. Estimates are that it takes six to 12 months to gain full compliance with CMMC 1.0 requirements.
2. Achieving CMMC Level 1 compliance builds upon the basic principles of cyber hygiene that must be completed first.
3. By ensuring that basic cyber hygiene principles are applied to the company's processes and procedures, ACME Consulting can position itself as a trusted 'supplier of choice' to gain future business.

7. Preliminary Level 1 Assessment Score

The CMMC 2.0 Level 1 scoring spreadsheet, located in Appendix A, was used to determine an initial Level 1 Assessment Score of 17% (10/59 objectives). This score was determined based on personnel interviews, an analysis of policies and procedures, and a network and physical security site walk-down. Scoring is on a scale of 0% to 100%, with 100% being the score necessary to achieve Level 1 compliance.

8. Executive Summary of Findings & Recommendations

A total of 15 specific cybersecurity practices composed of 59 objectives found in NIST SP 800-

171, Rev.2, must be implemented to achieve CMMC 2.0 Level 1 compliance. Appendix B provides a detailed determination regarding compliance with the 59 objectives of CMMC 2.0 Level 1. The following is a summary of the significant findings and recommendations related to this assessment.

Findings

The company lacks the necessary administrative, technical, and physical security controls in place to properly handle FCI per FAR 52.204-21 and NIST 800-171, which are required to pass a CMMC 2.0 Level 1 self-assessment.

The company lacks:

- formalized policies and procedures
- a consistent culture and practice of safeguarding FCI
- basic cyber hygiene practices
- a well-defined network infrastructure
- consistent and formalized network security practices

Overall, ACME Consulting needs more standardization, including a well-defined information technology and cybersecurity plan. Standardization is needed for email and anti-virus usage and for providing formalized policies and procedures to employees. A physical security plan is also necessary to proceed.

9. Support Organization Resources

ACME Consulting may choose to avail themselves of the following business resources that can assist with various aspects of achieving CMMC Level 1 as well as provide support towards attracting local, regional, state and local government contracts for which Level 1 protection of FCI is required.

- **APEX Accelerator | https://gtapexaccelerator.org/**
  Aileen Zoellner, CPP
  Government Certified Procurement Professional (CPP)
  Georgia Tech APEX Accelerator Counselor | Warner Robins Office
  Email: aileen.zoellner@innovate.gatech.edu | Mobile: 478-397-9138

- **Georgia Tech Manufacturing Extension Partnership | https://gamep.org/**
  Charity P. Stevens, Regional Manager, Central Region
  Office: 478.275.5125 | Mobile: 478.230.3945
  Email: charity.stevens@innovate.gatech.edu

10. Self-Assessment Reporting

An annual Level 1 self-assessment, with an accompanying senior company official affirmation of compliance, must be entered into the Supplier Performance Risk System (SPRS) asserting that ACME Consulting is meeting all the basic safeguarding requirements for FCI specified in FAR Clause 52.204-21. [Company Name Here] should use the self-assessment methods as defined in

the CMMC Self-Assessment Guide, Level 1, Version 2 (December 2021). Once ACME Consulting has self-assessed and finds they comply with all Level 1 practices, other entities (e.g., government sponsors and prime contractors looking to hire subcontractors) will have increased confidence in doing business with [Company Name].

ACME Consulting can choose to perform the annual self-assessment internally or engage a third-party to assist with evaluating their Level 1 compliance. A self-assessment is considered a low-confidence assessment by the DoD. Use of an independent third-party to perform an assessment is considered a moderate confidence assessment by the DoD. Either assessment and its result can be used to attest certification.

SECTION II – APPENDICES

APPENDIX A - CMMC Control Assessment Scoring Table

NIST SP 800-171A and the CMMC Self-Assessment Guide for Level 1 were used to verify and validate the status of the 15 practices at ACME Consulting.

To verify and validate that ACME Consulting is meeting CMMC practices, evidence needs to exist demonstrating that ACME Consulting has fulfilled the objectives of the Level 1 practices. Because different self-assessment objectives can be met in various ways (e.g., through documentation, computer configuration, network configuration, or training) a variety of techniques were used, including any and all of the three assessment methods described in NIST SP 800-171A (Examine, Interview or Test), to determine if [Enter Company Name] meets the intent of the Level 1 practices.

The assessment of a CMMC practice results in one of three possible findings: MET, NOT MET, or NOT APPLICABLE. To demonstrate CMMC Level 1 compliance, ACME Consulting will need a finding of MET or NOT APPLICABLE on all 17 Level 1 practices.

- **MET**: The contractor successfully meets the practice.
- **NOT MET**: The contractor has not met the practice.
- **NOT APPLICABLE (N/A)**: The practice does not apply for the self-assessment.

No.	NIST 800-171 Practice	Control Family	Control Text	Compliance Status MET/NOT MET
	Access Control (AC)			
1	AC.L1-b.1.i	Authorized Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	**NOT MET**

No.	NIST 800-171 Practice	Control Family	Control Text	Compliance Status MET/NOT MET
2	AC.L1-b.1.ii	Transaction & Function Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	NOT MET
3	AC.L1-b.1.iii	External Connections	Verify and control/limit connections to and use of external information systems.	NOT MET
4	AC.L1-b.1.iv	Control Public Information	Control information posted or processed on publicly accessible information systems.	NOT MET
	Identification and Authentication (IA)			
5	IA.L1-b.1.v	Identification	Identify information system users, processes acting on behalf of users, or devices.	NOT MET
6	IA.L1-b.1.vi	Authentication	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	NOT MET
	Media Protection (MP)			
7	MP.L1-b.1.vii	Media Disposal	Sanitize or destroy information system media containing FCI before disposal or release for reuse.	NOT MET
	Physical Protection (PE)			
8	PE.L1-b.1.viii	Limit Physical Access	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	NOT MET
9	PE.L1-b.1.ix	Manage Visitors & Physical Access	Escort visitors and monitor visitor activity, maintain audit logs of physical access, and control and manage physical access devices	NOT MET
	System and Communications (SC)			
10	SC.L1-b.1.x	Boundary Protection	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	NOT MET

No.	NIST 800-171 Practice	Control Family	Control Text	Compliance Status MET/NOT MET
11	SC.L1-b.1.xi	Public-Access System Separation	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	MET
	System and Information Integrity (SI)			
12	SI.L1-b.1.xii	Flaw Remediation	Identify, report, and correct information and information system flaws in a timely manner.	NOT MET
13	SI.L1-b.1.xiii	Malicious Code Protection	Provide protection from malicious code at appropriate locations within organizational information systems.	NOT MET
14	SI.L1-b.1.xiv	Update Malicious Code Protection	Update malicious code protection mechanisms when new releases are available.	NOT MET
15	SI.L1-b.1.xv	System & File Scanning	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	NOT MET

APPENDIX B - CMMC Rapid Assessment Scoring Spreadsheet

CMMC Level 1 include 17 practices and 59 objectives listed below.

Access Control		*MET*	*NOT-MET*
AC.L1-b.1.i Authorized Access Control			
	Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; account management compliance reviews; list of devices and systems authorized to connect to organizational systems.		
1	Authorized users are identified.	☒	☐
2	Processes acting on behalf of authorized users are identified.	☐	☒
3	Devices (and other systems) authorized to connect to the system are identified.	☐	☒
4	System access is limited to authorized users	☒	☐
5	System access is limited to processes acting on behalf of authorized users.	☒	☐
6	System access is limited to authorized devices (including other systems).	☐	☒
AC.L1-b.1.ii Transaction & Function Control			
	Access control policy; procedures addressing access enforcement; design documentation; list of approved authorizations including remote access authorizations; system configuration settings and associated documentation.		
7	The types of transactions and functions that authorized users are permitted to execute are defined.	☒	☐
8	System access is limited to the defined types of transactions and functions for authorized users.	☐	☒
AC.L1-b.1.iii External Connections			
	Access control policy; procedures addressing the use of external systems; terms and conditions for external systems; list of applications accessible from external systems; system configuration settings and associated documentation; system connection or processing agreements; account management documents.		
9	Connections to external systems are identified.	☐	☒
10	The use of external systems is identified.	☐	☒
11	Connections to external systems are verified.	☐	☒
12	The use of external systems is verified	☐	☒
13	Connections to external systems are controlled/limited.	☐	☒
14	The use of external systems is controlled/limited.	☐	☒
AC.L1-b.1.iv Control Public Information			

	Access control policy; procedures addressing publicly accessible content; list of users authorized to post publicly accessible content on organizational systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public websites; system audit logs and		
15	Individuals authorized to post or process information on publicly accessible systems are identified.	☒	☐
16	Procedures to ensure FCI is not posted or processed on publicly accessible systems are identified.	☐	☒
17	A review process is in place prior to posting of any content to publicly accessible systems.	☒	☐
18	Content on publicly accessible systems is reviewed to ensure that it does not include FCI.	☒	☐
19	Mechanisms are in place to remove and address improper posting of FCI.	☐	☒
Identification and Authentication		***MET***	***NOT-MET***
IA.L1-b.1.v Identification			
	Identification and authentication policy; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit logs and records; list of system accounts; other relevant documents or record		
20	System users are identified.	☐	☒
21	Processes acting on behalf of users are identified.	☐	☒
22	Devices accessing the system are identified.	☐	☒
IA.L1-b.1.vi Authentication			
	Identification and authentication policy; procedures addressing authenticator management; procedures addressing user identification and authentication; system design documentation; list of system authenticator types; system configuration settings and associated documentation; change control records associated with managing system authenticators; system audit logs and records; other relevant documents or records		
23	The identity of each user is authenticated or verified as a prerequisite to system access.	☐	☒
24	The identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access.	☐	☒
25	The identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.	☐	☒
Media Protection		***MET***	***NOT-MET***
MP.L1-b.1.vii Media Disposal			
	System media protection policy; procedures addressing media sanitization and disposal; applicable standards and policies addressing media sanitization; media sanitization records; system audit logs and records; system design documentation; system configuration settings and associated documentation; other relevant documents or records		

26	System media containing FCI is sanitized or destroyed before disposal.	☐	☒
27	System media containing FCI is sanitized before it is released for reuse.	☐	☒
Physical Protection		***MET***	***NOT-MET***
PE.L1-b.1.viii Limit Physical Access			
	Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; physical access list reviews; physical access termination records and associated documentation.		
28	Authorized individuals allowed physical access are identified.	☐	☒
29	Physical access to organizational systems is limited to authorized individuals.	☐	☒
30	Physical access to equipment is limited to authorized individuals.	☐	☒
31	Physical access to operating environments is limited to authorized individuals.	☐	☒
PE.L1-b.1.ix Manage Visitors & Physical Access			
	Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility.		
32	Visitors are escorted.	☐	☒
33	Visitor activity is monitored	☐	☒
34	Determine if audit logs of physical access are maintained.	☐	☒
35	Physical access devices are identified.	☐	☒
36	Physical access devices are controlled.	☐	☒
37	Physical access devices are managed.	☐	☒
Systems and Communications		***MET***	***NOT-MET***
SC.L1-b.1.x Boundary Protection			
	System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the system; system design documentation; boundary protection hardware and software; enterprise security architecture documentation; system audit logs and records; system configuration settings and associated documentation.		
38	The external system boundary is defined.	☐	☒
39	Key internal system boundaries are defined.	☒	☐
40	Communications are monitored at the external system boundary.	☐	☒
41	Communications are monitored at key internal boundaries.	☒	☐
42	Communications are controlled at the external system boundary.	☐	☒
43	Communications are controlled at key internal boundaries.	☐	☒
44	Communications are protected at the external system boundary.	☐	☒

45	Communications are protected at key internal boundaries	☐	☒
SC.L1-b.1.xi Public-Access System Separation			
	System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the system; system design documentation; boundary protection hardware and software; system configuration settings and associated documentation; enterprise security architecture documentation.		
46	Publicly accessible system components are identified.	☒	☐
47	Subnetworks for publicly accessible system components are physically or logically separated from internal networks.	☒	☐
System and Information		***MET***	***NOT-MET***
SI.L1-b.1.xii Flaw Remediation			
	System and information integrity policy; procedures addressing flaw remediation; procedures addressing configuration management; list of flaws and vulnerabilities potentially affecting the system; list of recent security flaw remediation actions performed on the system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct system flaws); test results from the installation of software and firmware updates to correct system flaws; installation/change control records for security-relevant software and firmware updates.		
48	The time within which to identify system flaws is specified.	☐	☒
49	System flaws are identified within the specified time frame	☐	☒
50	The time within which to report system flaws is specified.	☐	☒
51	System flaws are reported within the specified time frame.	☐	☒
52	The time within which to correct system flaws is specified.	☐	☒
53	System flaws are corrected within the specified time frame	☐	☒
SI.L1-b.1.xiii Malicious Code Protection			
	System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; records of malicious code protection updates; malicious code protection mechanisms; system configuration settings and associated documentation; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; scan results from malicious code protection mechanisms; system design documentation.		
54	Designated locations for malicious code protection are identified.	☐	☒
55	Protection from malicious code at designated locations is provided.	☐	☒
SI.L1-b.1.xiv Update Malicious Code Protection			
	System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection.		

56	Determine if malicious code protection mechanisms are updated when new releases are available.	☐	☒
SI.L1-b.1.xv System & File Scanning			
	System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection.		
57	The frequency for malicious code scans is defined.	☐	☒
58	Malicious code scans are performed with the defined frequency.	☐	☒
59	Real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.	☐	☒

APPENDIX C – Findings

AC.L1-b.1.i Authorized Access Control

Employees are only permitted to access company email on their personal devices; however, several weaknesses are evident in this approach. Logs of recent system and email access are not documented, making it difficult to monitor or review user activity. The owner is the only person with access to company portals, and the policy for employee access what said to be “different” with no further explanation. There is no further information on what employees have access to other than their email. On the topic of devices, there is no record of what devices employees use to access company portals from home, and there is no policy for whether former employees' devices are wiped or not upon leaving the organization. Although employee and owner accounts are the only ones with explicit access to the company’s systems, the lack of any authentication like MFA makes it hard to confidently say that their system is secure enough to ensure users are who they say who they are.

AC.L1-b.1.ii Transaction and Function Control

Employees are only permitted to access company email on their personal devices; however, several weaknesses are evident in this approach. Logs of recent system and email access are not documented, making it difficult to monitor or review user activity. There is also no clear indication of which actions are allowed versus disallowed, raising questions about whether employees can download attachments or automatically forward emails to personal accounts. Additionally, there is no evidence of a formal written policy, such as an access control policy or system security plan, that clearly defines approved authorizations. Finally, there is no auditing process in place to confirm that any restrictions are functioning as intended.

AC.L1-b.1.iii External Connections

All employee work is done via connection to external systems, which are their personal devices. However, the CMMC requirement is that this practice be well documented and written down, which is not the case here – in this scenario, this is just the way it’s done due to small company size. Similarly, there is no documentation as to what they are allowed to do on their external devices. Since these are their personal devices, in theory they have free reign to access anything they want and do anything they want with the data on them. By nature of it being their personal devices, there is no true control/limit over what employees can do with these systems; there is nothing in place such as VPN to manage these. Furthermore, it is mentioned that while on travel, all access to the internet is done over public internet, which makes such external connections unmanaged. Even though the IT scans/sanitizes a device initially for bugs, there is no continuous system in place that monitors what takes place on these devices while they are actually in use.

AC.L1-b.1.iv – Control Public Information

While the company owner currently maintains sole access to public information platforms, there are no formally documented procedures governing the review, approval, and posting of public content. The absence of defined controls introduces risk in the event of miscommunication or future delegation of

access to additional personnel, potentially resulting in noncompliance with required review and authorization standards.

IA.L1-b.1.v Identification

While employees are given a unique company email to log into their email, these accesses are not recorded in an audit log of any form. These logins are through Microsoft 365, but it is not specified whether the logins are stored or kept as a record of any form. Since there is no audit logging functionalities currently implemented, user processes and devices are not kept in any record either. The company uses personal devices, and users are allowed to log in on any personal devices that they choose, including cell phones. The devices themselves are never uniquely identified, nor are any associated user processes. Since users, processes, and devices are not uniquely identified and logged, all three objectives in this control are not met.

IA.L1-b.1.vi Authentication

The company's existing policies and procedures do not address authentication or authenticator management. Employees can access company systems via Microsoft 365 on personal devices with no MFA, no VPN, and no device verification requirements. Nothing in the provided documentation addresses how processes acting on behalf of users are authenticated. Additionally, no documentation regarding authenticator management, system configuration, or audit logs was provided. Since user, process, and device authentication and verification are not prerequisites for system access, objectives 23, 24, and 25 are all NOT MET.

MP.L1-b.1.vii Media Disposal

The company has no formal procedure to dispose of FCI on company devices. The company follows a BYOD model, meaning employees have access to FCI on their own company devices. The company stated that when employees are terminated, their emails are also terminated; however, the company never stated that it would also remove FCI from the employee devices after termination. Furthermore, the company has not yet established a rigid plan, stating that no employees have been terminated as of the mock assessment. Overall, since there was no official and formal plan stated by the company regarding the removal of FCI information from company employee devices, this control is not met.

PE.L1-b.1.viii Limit Physical Access

The company has no physical and environmental protection policy or documented procedures addressing physical access authorizations. No authorized personnel access list exists identifying who is allowed physical access to systems, equipment, or operating environments; the owner verbally claims sole access but no documentation supports this. The BYOD model places company information on personal devices the organization cannot physically control, and as a fully remote company, operating environments extend to every employee's home with no method for controlling access in those environments.

PE.L1-b.1.ix Manage Visitors & Physical Access

The company's existing policies and procedures do not include a physical and environmental protection policy, or any documented procedures addressing physical access control. The company has no documented process for escorting visitors or monitoring visitor activity, and the only physical monitoring mentioned is a Ring camera that the owner confirmed has no backups and provides no meaningful physical security. No audit logs of physical access are maintained or reviewed, as the owner stated there is no regular audit process, and IT is engaged only on request with no active monitoring. Physical access devices are neither identified, controlled, nor managed; there is no inventory of access devices or entry points, employee BYOD equipment is untracked throughout its lifecycle, and former employee accounts and devices remain in an unknown state post-offboarding with no confirmation of device recovery or data wipe.

SC.L1-b.1.x – Boundary Protection

The organization demonstrates significant deficiencies in boundary protection controls due to the use of a Bring Your Own Device (BYOD) model and reliance on public Wi-Fi networks. The use of unmanaged personal devices limits the organization’s ability to enforce security controls, monitor user activity, or ensure compliance with security policies. Additionally, connecting to public Wi-Fi networks increases exposure to external threats, effectively expanding the network boundary to the public internet and elevating the risk of unauthorized access and data compromise.

SC.L1-b.1.xi Public-Access System Separation

The organization has implemented separation between publicly accessible systems and its internal network in accordance with SC.L1-b.1.xi. A publicly accessible landing page was identified that serves a purely informational purpose, along with the organization’s LinkedIn presence. These external-facing components are logically separated from internal systems and networks, ensuring that public access does not introduce risk to sensitive or operational environments. This separation helps reduce the attack surface and prevents unauthorized access to internal resources through publicly available platforms.

SI.L1-b.1.xii Flaw Remediation

The company uses Microsoft 365 operating system for their computers, which comes with Microsoft Defender and optionally a more in-depth business plan. Microsoft Defender provides real-time protection against malware, ransomware, and phishing. The business plan also includes a dashboard to monitor flaws, identify vulnerabilities and track incidents. This alone does not comply with SI.L1-b.1.xii since it requires the necessary policies and procedures surrounding the software. These policies include defining the timeframe to identify, report, fix flaws in the system. The company does not define these policies, and therefore can not pass this control.

SI.L1-b.1.xiii Malicious Code Protection

The BYOD policy for employee devices vastly weakens the attempt at implementing malicious code protection via Microsoft Defender. Microsoft Defender is a rudimentary antiviral measure, and although it may provide limited malicious code protection, it is subject to modification or deactivation since each employee owns and carries their own device(s). Additionally, since a solution is only deployed for emails, there is not comprehensive security at all reasonable entry points for malicious code.

SI.L1-b.1.xiv Update Malicious Code Protection

Because there are no policies or mechanisms for protection against malicious code in place, there are also no documentation or mechanisms for updating it. Hence, the company fails this control.

SI.L1-b.1.xv System & File Scanning

The company has not defined a frequency for malicious code scans at the organizational level. The owner stated he runs antivirus scans on his own device on a personal basis, but no written policy establishes a scan frequency for the organization and there is no requirement for employees to perform scans on the personal devices they use for company work. Microsoft Defender is the stated antivirus and Microsoft 365 performs scanning within the cloud environment, but because employees use personal devices under a BYOD model, the organization has no visibility into whether real-time scanning is enabled on the endpoints where files are downloaded, opened, or executed.

APPENDIX D - NIST SP 800-171 Control Category Definitions and Clarification

Several of the terms in the self-assessment can be confusing. Companies who have performed self-assessments often misinterpret terms and therefore score their compliance incorrectly or disagree with an assessor's finding. The following are some of those terms along with their definition. These definitions may assist in determining why the assessor rated a control as a "no."

AC.L1-3.1.1 Authorized users.

The very first practice is to control access to your network by assigning all users unique usernames and passwords and having a user provisioning and deprovisioning process. This ensures only authorized personnel are allowed access to the network and services. While user access is the focus of this control, the practice and examples also mention controlling device access. You should distribute a statement to all staff that you will disable and remove unauthorized devices from the network, and that IT must authorize all devices before they can be connected.

Control who can use company computers and who can log on to the company network. This includes full-time and part-time employees, 3rd parties, managed service providers, interns, assessors, etc. Limit the services and devices, like printers, that can be accessed by company computers. Set up your system so that unauthorized users and devices cannot get on the company network.

AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL

This practice limits what authorized users can *do* once they're in the system, not just whether they can get in. Even after a user is identified and authenticated, they should only be able to perform the specific transactions and functions required for their job, the principle of least privilege applied to actions. For example, a sales employee may need to read customer records but should not be able to delete them, and a help desk technician should be able to reset passwords without having full administrator rights. To implement this, group users into roles based on job function and use the role-based access control features built into your operating systems, cloud platforms, and applications to enforce those permissions technically rather than relying on policy alone.

AC.L1-3.1.20 External Connections

External systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls or the determination of the effectiveness of implemented controls on those systems. External systems include personally owned systems, components, or devices and privately owned computing and communications devices [Enter Company Name] in commercial or public facilities. This requirement also addresses the use of external systems for the processing, storage, or transmission of FCI or CUI, including accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational systems.

Organizations establish terms and conditions for the use of external systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum, the types of applications that can be accessed on organizational systems from external systems. If terms and

conditions with the owners of external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

This requirement recognizes that there are circumstances where individuals using external systems (e.g., contractors, coalition partners) need to access organizational systems. In those situations, organizations need confidence that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been effectively implemented can be achieved by third-party, independent assessments, attestations, or other means, depending on the assurance or confidence level required by organizations.

Note that while "external" typically refers to outside of the organization's direct supervision and authority, that is not always the case. Regarding the protection of FCI/CUI across an organization, the organization may have systems that process FCI/CUI and others that do not. And among the systems that process FCI/CUI there are likely access restrictions for FCI/CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered "external" to that system.

To clarify, you may have external resources, such as cloud providers, which the organization utilizes and must be approved for use and managed. Larger organizations may also implement internal controls which limit access to certain areas of your network to certain users/devices, but those will be better defined in other practices. Your policies should state that the organization will verify and control/limit connections to, and use of, external information systems, and that only approved company devices are permitted access to company information systems and resources. Your plan will note any steps taken to ensure only company devices are used on the network, such as making devices enroll in Active Directory and any approved cloud service provider, or other external resource. The organization will measure the effectiveness of the plan by periodic internal scans of the network for unauthorized devices and review of logs from proxy servers, filters, or other internet access monitoring systems.

AC.L1-3.1.22 Control Public Information

In accordance with laws, Executive Orders, directives, policies, regulations, or standards, the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, FCI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Individuals authorized to post FCI onto publicly accessible systems are designated. The content of information is reviewed prior to posting onto publicly accessible systems to ensure that nonpublic information is not included.

In other words, do not allow FCI/CUI to become public, always safeguard the confidentiality of FCI/CUI by controlling the posting of FCI/CUI on company-controlled websites or public forums, and the exposure of FCI/CUI in public presentations or on public displays. It is important to know which users are allowed to publish information on publicly accessible systems, like your company website, and implement a review process before posting such information. If FCI/CUI is discovered on a publicly accessible system, procedures should be in place to remove that information and alert the appropriate parties.

IA.L1-3.5.1 Identification

Before a system can decide whether to let someone in, it has to know *who* is asking. This practice requires that every user, every process running on behalf of a user, and every device connecting to the system have a unique identifier. Shared accounts (a single "admin" or "frontdesk" login used by multiple people) violate this practice because they make it impossible to trace activity back to a specific individual. Each employee, contractor, and service account should have its own dedicated username, and default identifiers that ship with hardware or software (such as "admin" or "root") should be renamed or disabled where possible. Identification is the foundation that authentication builds on, without unique IDs, audit logs and accountability become meaningless.

IA.L1-3.5.2 Authentication

Identification answers "who are you," and authentication answers "prove it." This practice requires the system to verify the claimed identity of users, processes, and devices before granting access. The most common form is a password, but authentication can also include PINs, smart cards, biometrics, cryptographic keys, or tokens, whatever method is used must give reasonable confidence that the entity is who it claims to be. In practice, this means requiring strong passwords, changing default passwords on new equipment immediately, and protecting stored credentials from theft. Although CMMC Level 1 does not explicitly require multi-factor authentication (that's a Level 2 requirement), implementing MFA wherever practical greatly strengthens this control.

MP.L1-3.8.3 Media Disposal

This practice requires that any system media containing FCI be sanitized or destroyed before disposal, release for reuse, or transfer outside organizational control. "Media" includes both digital media (hard drives, SSDs, USB flash drives, backup tapes, CDs/DVDs) and paper documents. The risk is well-documented: discarded equipment is a recurring source of data breaches, with sensitive information regularly recovered from drives sold on auction sites or pulled from trash bins. Simply deleting files or formatting a drive is *not* sufficient, acceptable methods include overwriting with sanitization software, degaussing magnetic media, or physical destruction through shredding or crushing. For paper records, cross-cut shredding or a certified destruction service is appropriate, and the same standards should apply when media is being repurposed internally to a user without need-to-know.

PE.L1-3.10.1 Limit Physical Access

This practice requires that physical access to information systems, equipment, and the operating environments where they reside be limited to authorized individuals. The reasoning is straightforward: most technical controls can be bypassed if an attacker has physical access to a machine, they can boot from external media, clone hard drives, install hardware keyloggers, or simply steal the device. This control isn't just about the front door of your building; it includes server rooms, network closets, wiring rooms, and any space where equipment that handles FCI is located. In practice, this typically involves locked doors, badge or key access, separation of sensitive equipment from general-access areas, and regular review of who currently has access so that former employees or contractors no longer retain it.

PE.L1-3.10.3 Escort Visitors

This practice requires that visitors be escorted and their activity monitored while they are in areas where FCI is processed, stored, or transmitted. A "visitor" is anyone who is not an authorized member of the organization with regular access to that space, guests, vendors, delivery personnel, repair technicians, and even employees from other parts of the company who don't normally work there. The goal is to ensure no unaccompanied person can wander into a server room, sit at an unattended workstation, or photograph sensitive materials. In practice, escorting means a designated employee remains with the visitor for the entire duration, and monitoring means actively watching what they do, not just being in the same building. Maintenance workers, cleaning crews, and IT vendors should never be left alone in spaces with active FCI workstations or servers.

PE.L1-3.10.4 Physical Access Logs

This practice requires that audit logs of physical access be maintained, creating a record of who entered controlled areas and when. The intent is to provide investigative evidence if an incident occurs, without a log, an organization has no way to determine whether a particular person was in the server room when a hard drive went missing, or whether a visitor accessed an area outside their escorted scope. Logs can take many forms: an electronic badge access system, a paper visitor sign-in sheet, or a logbook at the entrance to a server room. Whatever method is used, the log should capture at minimum the identity of the person, the date, and the time of entry, with exit time recorded ideally as well. Logs should be retained for a defined period and protected from tampering, and they should cover both employees and visitors entering FCI-relevant spaces.

PE.L1-3.10.5 Manage Physical Access

To comply with this control, companies must identify all the areas within their physical premises that they want to block unauthorized individuals from accessing. This could include rooms, building floors, network infrastructure, server rooms, and computers and laptops. Then, only authorized staff or third parties who need physical access to do their jobs should be allowed to contact these spaces. To effectively limit physical access control, companies can use biometrics, badge readers, key cards, human guards, and so on.

This control also refers to physical devices: locks, keys, lock combinations, card readers, etc. Such devices only offer protection if companies know who has them and what level of physical access devices they’re configured to permit. Therefore, companies need to manage who can physically access them carefully. Ensuring employees leaving the organization turn in their ID and office keys, disabling old badges, etc., are also primary considerations.

Companies should implement appropriate Access Control policies and procedures to comply with these controls, such as background checks, employee training, employee off-boarding, and a strong visitor management program. Companies should also monitor secured areas of their physical environment for any signs of unauthorized access or suspicious activity.

SC.L1-3-13-1 Boundary Protection

Communications can be monitored, controlled, and protected at boundary components and by restricting or prohibiting interfaces in organizational systems. Boundary components include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a system security architecture (e.g., routers protecting firewalls or application gateways on protected subnetworks). Restricting or prohibiting interfaces in organizational systems includes restricting external web communications traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.

Organizations consider the shared nature of commercial telecommunications services in the implementation of security requirements associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. NIST SP 800-41 provides guidance on firewalls and firewall policy. NIST SP 800-125B provides guidance on security for virtualization technologies.

Fences, locks, badges, and key cards help keep non-employees out of your physical facilities. Similarly, your company's IT network or system has boundaries that must be protected. Many companies use web proxies and a firewall.

When an employee uses a company computer to go to a website, a web proxy makes the request on the user's behalf, looks at the web request, and decides if it should let the employee go to the website. A firewall controls access from the inside and outside, protecting valuable information and resources stored on the company's network. A firewall stops unwanted traffic on the internet from passing through an outside "fence" to the company's networks and information systems. Internal boundaries determine where data can flow, for instance a software development environment may have its own boundary controlling, monitoring, and protecting the data that can leave that boundary.

You may want to monitor, control, or protect one part of the company network from another. This can also be accomplished with a firewall and limits the ability of attackers and disgruntled employees from entering sensitive parts of your internal network and causing damage.

SC.L1-3.13.5 Public-Access System Separation

Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs). DMZs are typically implemented with boundary control devices and techniques that include routers, gateways, firewalls, virtualization, or cloud based technologies. NIST SP 800-41 provides guidance on firewalls and firewall policy. SP 800-125B provides guidance on security for virtualization technologies.

Separate the publicly accessible systems from the internal systems that need to be protected. Do not place internal systems on the same network as the publicly accessible systems and block access by default from DMZ networks to internal networks.

One method of accomplishing this is to create a DMZ network, which enhances security by providing public access to a specific set of resources while preventing connections from those resources to the

rest of the IT environment. Some contractors achieve a similar result through the use of a cloud computing environment that is separated from the rest of the company's infrastructure.

SC.L2-3-13-6 Network Communication by Exception

This requirement applies to inbound and outbound network communications traffic at the system boundary and at identified points within the system. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

Block all traffic entering and leaving the network, but permit specific traffic based on organizational policies, exceptions, or criteria. This process of permitting only authorized traffic to the network is called whitelisting and limits the number of unintentional connections to the network.

This practice, SC.L2-3.13.6, requires a deny-all permit by exception approach for all network communications. In doing so, it adds specifics for SC.L1-3.13.1, which only requires monitoring, control, and protection of communication channels.

SI.L1-3.14.1 - Flaw Remediation

This practice requires that information system flaws, software vulnerabilities, bugs, and misconfigurations, be identified, reported, and corrected in a timely manner. Most commonly this refers to security vulnerabilities in operating systems, applications, firmware, and network devices that vendors release patches to fix. Timeliness genuinely matters: attackers actively scan the internet for known unpatched vulnerabilities, and the time between a patch being released and exploits appearing in the wild is often measured in days or hours. In practice, this means establishing a process for learning about flaws (vendor notifications, vulnerability scans, security advisories), evaluating which ones apply to your environment, and applying fixes within a reasonable timeframe based on severity, critical patches warrant rapid deployment, while lower-severity updates may follow a regular monthly schedule. The organization should keep some record of which systems were patched and when.

SI.L1-3.14.2 - Malicious Code Protection

Provide protection from malicious code at appropriate locations within organizational information systems. Concerning locations which should be designated with respect to the first objective for this control: Any system component which can be reasonably considered as a potential avenue for malicious code to enter and infect the system should be identified as a point where malicious code protection should be applied.

SI.L1-3.14.4 - Update Malicious Code Protection

This practice requires that malicious code protection mechanisms be updated when new releases are available. Anti-malware tools are only as good as the threat intelligence they have, a virus scanner with year-old signatures will miss the threats that have emerged since. Modern endpoint protection tools update both their signature databases (the lists of known threats) and their detection engines (the software that does the scanning), often multiple times per day, and both kinds of updates matter. In practice, the simplest reliable approach is enabling automatic updates so signature and engine updates are pulled down without manual intervention, and periodic verification that endpoints are actually receiving them, update mechanisms can silently fail. Devices that are offline for extended periods or personally owned under a BYOD model are common gaps.

SI.L1-3.14.5 - System & File Scanning

This practice requires periodic scans of the information system, along with real-time scans of files from external sources as those files are downloaded, opened, or executed. The two scan types serve different purposes: periodic full-system scans catch malware that may have slipped past initial defenses or was dormant when it first arrived, while real-time scanning catches threats at the moment they enter the system, before they have a chance to execute. In practice, periodic scans are typically scheduled to run weekly or daily during off-hours so they don't disrupt user work, while real-time scanning runs continuously in the background and inspects files as they are accessed. "External sources" includes email attachments, web downloads, USB drives, cloud storage syncs, and files received through messaging applications. Most modern endpoint protection products perform both by default, but the organization should confirm both are actually enabled, real-time scanning is sometimes disabled by users who find it slows their machine, which defeats the protection.

Disclaimer Statement

The content and information contained in this Cybersecurity Assessment is provided as is and based on reasonable research efforts. Georgia Institute of Technology ("Georgia Tech") makes no representations or warranties of any kind, express or implied, regarding, but not limited to, the accuracy, completeness, timeliness, utility, suitability, reliability or availability with respect to such content, information or services provided in connection therewith. Your use of or reliance on this Cybersecurity Assessment or the content or information contained herein or services provided in connection therewith are strictly at your own risk.

Georgia Tech shall not be liable under any circumstances, directly or indirectly, for any damage or loss of any kind, regardless of whether they have been advised of the possibility of such loss or damages, including but not limited to, direct, indirect, special, incidental or consequential loss or damage, arising from, caused or alleged to be caused by or in connection with any use of or reliance on this Cybersecurity Assessment or the content or information contained herein or services provided in connection therewith.

ALL WARRANTIES AND REPRESENTATIONS, WHETHER EXPRESSED, IMPLIED OR STATUTORY, REGARDING THIS CYBERSECURITY ASSESSMENT AND THE CONTENT OR INFORMAITON CONTAINED HEREIN OR SERVICES PROVIDED IN CONNECTION THEREWITH ARE EXPRESSLY DISCLAIMED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF PERFORMANCE, MERCHANTIABILITY, FITNESS FOR A PARTICULAR USE OR PURPOSE, NONINFRINGEMENT OR WARRANTY THAT THE ASSESSMENT, CONTENT, INFORMATION OR SERVICES PROVIDED ARE ERROR FREE.

For avoidance of doubt, Georgia Tech includes its Enterprise Innovation Institute ("EI^2") and Georgia Manufacturing Extension Partnership ("GaMEP") as well as The Board of Regents of the University System of Georgia ("BOR") and our respective affiliated organizations and individual members, officers, trustees, directors, employees, agents and representatives.