Preliminary Analysis of CMMC v0.6

A Green Paper: Analysis of The DoD Cybersecurity Maturity Model Certification (CMMC) v0.6 Soliciting Input and Comments

Analysis and comments on the CMMC v0.6 (which only includes Levels 1 through 3) are provided. The total number of practices and compliance items have been substantially reduced (through Level 3) and now are only modestly higher than than the number of requirements in NIST800-171. The use of referenced security requirements and controls have been clarified, and now reference cybersecurity progrms from Australia and the United Kingdom. Information regardeing Levels 4 & 5 has not been released nor has work classification by level been provided.

Abstract

Michael G. Semmens
President & CEO, Imprimis Inc.
Chairman, National Cyber Exchange

Steve Lines
President DIB ISAC Inc.

Jennifer Kurtz
Cyber Program Director
Manufacturer's EDGE

BLUF (Bottom Line Up Front)

The CMMC drafts have changed significantly between v0.4 and v0.6. Although only levels 1-3 were published, it is clear that the size and content have been shaped to make primary use of NIST SP 800-171 at level 3 as promised by OSD. Key takeaways from v0.6 are:

1. The number of practices and processes has been dramatically reduced as has been the number of cited security controls and requirements from other frameworks and standards.
2. Clarification was provided that cited controls and requirements such as NIST 800-171, CSF or CIS v7.1 are used to "inform" the practices defined in CMMC v0.6 and are references and NOT requirements for compliance. The Australian Cyber Security Centre or ACSC Essential 8 Maturity Model and the UK NCSC (United Kingdom National Cyber Security Centre) Essentials were added as cited or referenced material.
3. The Governance Domain has been deleted and policy and governance has been integrated into the five maturity processes required through level 3.
4. The practices of CMMC, in fact, follow the cited references very closely so implementing the CMMC practices effectively implements the cited reference, and vice versa, particularly in the case of NIST 800-171.
5. Implementing all requirements defined in NIST 800-171 satisfies the overwhelming majority of the CMMC practices through level 3 as defined in CMMC v0.6.
6. There are a total of 21 practices contained within CMMC v0.6 that do not have reference to NIST 800-171 and are therefore additional requirements.

The CMMC does not represent a huge change from NIST 800-171 but does add some important practices that do bring value to the security baseline. The big questions remain. First, what category of work or contract can be performed at the various maturity levels or conversely, what is the level of procurement activity each level will earn? It still appears that level 3 is the first meaningful certification level. The second question is how and when will certification happen? OSD is actively developing the certification program and details should be available soon. The key takeaway for DoD contracting companies is that certification will happen and soon.

Let us know what you think. Submit comments to https://nationalcyber.org/CMMC and the DIB ISAC and the NCX will make sure all comments are received by the CMMC team.

Preliminary Analysis of CMMC v0.6

A Green Paper: Analysis of The DoD Cybersecurity Maturity Model Certification (CMMC) for Submittal

This paper builds on the analysis performed in the previous effort which analyzed the CMMC v0.4. This paper (Reference 1) can be obtained at https://natioanlcyber.org/CMMC . It summarizes the impetus for CMMC, and provides a detailed analysis of the practices, processes, and ACIs (Additional Compliance Items) contained in version 0.6.

CMMC PRACTICES, PROCESSES, AND REFERENCED COMPLIANCE ITEMS

The CMMC v0.6 indicates a shaping of the standard to closely align with the NIST SP 800-171. In fact, at level 3 it can be accurately referred to as "171+21." The practices reference NIST 800-171 requirements in the overwhelming majority of practices and they closely align in both intent and content. There are a total of 21 practices that have been included in the CMMC that do not refer to a NIST 800-171 requirement.

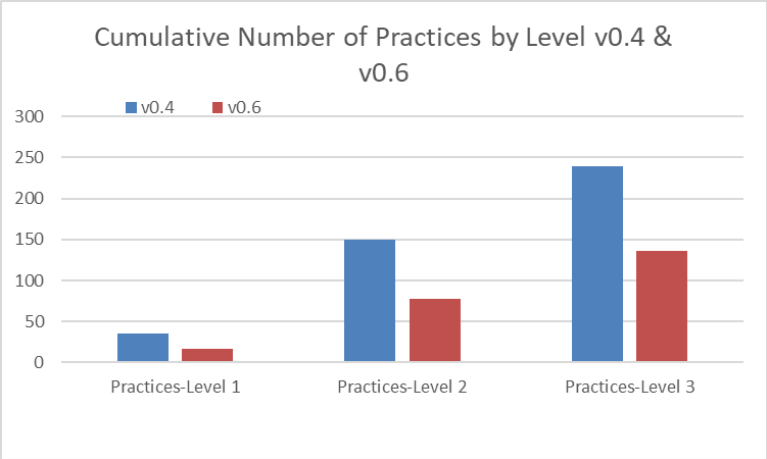

Figure 1 Number of Practices CMMC v0.4 & v0.6+

The comparison of the total number of practices between the two versions of CMMC are shown in Figure 1. The number of cited controls and requirements is shown in Figure 2. The number of practices and processes by level and domain is shown in Figure 3.

There has been an almost 50% reduction in the number of practices and cited controls. The trimming by the authors was done in such a way that NIST 800-171 is the dominant standard at level 3, just as promised by OSD.

As can be seen in Figure 3, the domains have been slightly trimmed to 17 dropping Cybersecurity Governance, the total number of Capabilities remain at 40 and there are 131 practices and 5 maturity processes.

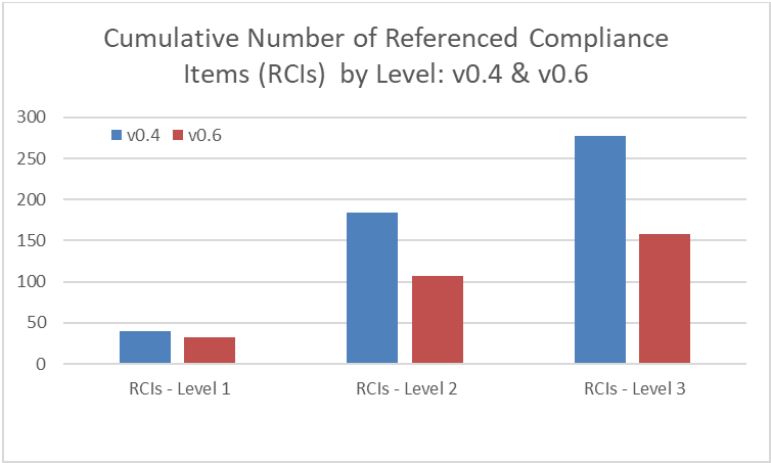

Figure 2 CMMC Referenced Compliance Items

	CMMC Domains	Capabilities Total	Practices Total	LEVEL 1	LEVEL 2	LEVEL 3	TOTALS
				Practices	Practices	Practices	Practices Total
1	Acces Control (AC)	4	22	4	12	6	22
2	Asset Management (AM)	1	2	0	0	2	2
3	Audit & Accountability (AA)	4	11	0	4	7	11
4	Awareness & Training (AT)	2	3	0	2	1	3
5	Configuration Management (CM)	2	9	0	6	3	9
6	~~Cybersecurity Governance (CG)~~						
7	ID & Authorization (IDA)	1	11	2	5	4	11
8	Incident Response (IR)	5	7	0	5	2	7
9	Maintenance (MA)	1	6	0	4	2	6
10	Media Protection (MP)	4	8	1	3	4	8
11	Personnel Security (PS)	2	2	0	2	0	2
12	Physical Protection (PP)	1	6	4	1	1	6
13	Recovery (RE)	1	3	0	2	1	3
14	Risk Management (RM)	2	6	0	3	3	6
15	Security Assessment (SAS)	3	5	0	3	2	5
16	Situational Awareness (SA)	1	1	0	0	1	1
17	System & Comms Protection (SCP)	2	19	2	3	14	19
18	System & Info. Integrity (SII)	4	10	4	3	3	10
	Practices TOTALS	40	131	17	58	56	131
	Maturity Processes TOTALS		5	0	3	2	5
	Practices & Maturity Processes ACCUMULATIVE TOTALS	40	136	17	78	136	136

Figure 4 CMMC Capabilities and Practices by Level and Domain

Level 1 includes 17 practices which align with NIST 800-171 and the FAR 52.204-21. The FAR clause contains 15 requirements which aligns – nearly verbatim – to the requirements contained in NIST 800-171 where 3 of the 171 requirements were combined into a single FAR requirement. The full comparison of FAR and NIST requirements is provided in Appendix A. Level 1 addresses all of the FAR requirements – another promise kept by OSD. Level 2 is a substantial increase over level 1

	LEVEL 1	LEVEL 2	LEVEL 3
NIST 800-171	17	51	42
RMM	13	18	4
ISO 27001:2013	0	1	1
CSF	1	2	0
CIS	1	3	5
TOTALS	32	75	52

Figure 3 Cited Security Controls and Requirements by Framework

with 58 practices and 3 maturity processes, and level 3 includes practices that cite all 110 requirements of NIST 800-171.

	LEVEL 1	LEVEL 2	LEVEL 3	TOTAL	% OF TOTAL
NIST 800-171	17	68	110	110	69%
RMM	13	31	35	35	22%
ISO 27001:2013	0	1	2	2	1%
CSF	1	3	3	3	2%
CIS	1	4	9	9	6%
TOTALS	32	107	159	159	100%

Figure 5 Cumulative Number of Cited Security Controls

The standards or framework requirements or controls cited by CMMC are shown in Figure 4 and 5 below. Nearly 70% of the cited controls pertain to NIST 800-171, about 1 in 5 cite the Carnegie Mellon CERT RMM (Resilence Management Model) practices, and less than 10% are from other frameworks.

The alignment of the CMMC practices and the cited standard/framework requirements or controls is illustrated by the samples shown in Figure 6. The CMMC practices and cited references are shown in the

Figure 6 Sample Alignment of Practices & Controls

	Domain: Access Control AC/C001		**Domain: Configuration Management CM/C013**
	Level 1	Level 2	Level 2
CMMC	P1001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). • FAR Clause 52.204-21 b.1.i • NIST SP 800-171 3.1.1 • AU ACSC Essential Eight	P1005 Provide privacy and security notices consistent with applicable Federal Contract Information rules. • NIST SP 800-171 3.1.9	P1061 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. • NIST SP 800-171 3.4.1 • CERT RMM v1.2 KIM:SG5.SP2 • UK NCSC Cyber Essentials
FAR	(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).		
CERT RMM v1.2			KIM:SG5 Manage Information Asset Integrity KIM:SG5.SP2 Manage Information Asset Configuration Information asset baselines are created and changes are managed.
NIST 800-171	3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	3.1.9 Provide privacy and security notices consistent with applicable CUI rules.	3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

first row of the figure. The cited reference is provided in the rows below. The language of the CMMC practice and the controls cited show strong alignment and in some case exact alignment. This shows that the CMMC is well grounded in Information Assurance practices which opens up a large body of knowledge to support the execution of the CMMC.

The Australian Cyber Security Centre or ACSC Essential 8 Maturity Model and the UK NCSC (United Kingdom National Cyber Security Centre) Essentials are cited multiple times through the first three levels. Each represents an entire program established by the respective governments that focus on the implementation of information security core competencies. The high level summary is provided in the table below. They are both consistent with the classical information security core competencies but the genius is within the simplicity of their approach, not overwhelming the end users.

AU ACSC Essentials https://www.cyber.gov.au/	UK NCSC https://www.cyberessentials.ncsc.gov.uk/
Mitigation Strategies to Prevent Malware Delivery and Execution 1. Application Whitelisting 2. Configure Microsoft Office Macro Settings 3. Patch Applications 4. User Application Hardening Mitigation Strategies to Limit the of Cyber Security Incidents 5. Restrict Administrative Privileges 6. Multi-Factor Authentication 7. Patch Operating Systems Mitigation Strategies to Recover Data and System Availability 8. Daily Backups	1. Secure Internet Connection 2. Secure Devices and Software 3. Control Access to Data and Services 4. Protect from Viruses and Other Malware 5. Keep Devices and Software Up to Date

NEW PRACTICES

A total of 21 practices are included in the CMMC v0.6 that do not refer to a NIST 800-171 requirement. These 21 practices are distributed over 9 domains:

1. Asset Management (AM) – 2
2. Audit and Accountability – 2
3. Incident Response (IR) – 4
4. Recovery (RE) – 2
5. Risk Management – 3
6. Security Assessment (SAS) – 1
7. Situational Awareness (SA) – 1
8. System & Communications Protection (SCP) – 3
9. System & Information Integrity (SII) - 3

These practices are shown in Figure 7. The first two categories enhance CUI marking and management and call for a centralized log reposity and reviews of audit logs. Four practices are added in the Incident Response (IR) domain calling for triage of events and root cause analysis. The two practices added to the Recovery (RE) domain require backups and the storage of backups off-site on a periodic basis.

Figure 7 Additional Practices Beyond NIST 800-171

	CMMC Domains	#	New Practices Added
1	**Acces Control (AC)**	***0***	*None*
2	**Asset Management (AM)**	**2**	**P1035** Identify, categorize, and label all CUI data; **P1036** Define procedures for the handling of CUI data.
3	**Audit & Accountability (AU)**	**2**	**P1048** central log repository; **P1044** Review audit logs
4	**Awareness & Training (AT)**	***0***	*None*
5	**Configuration Management (CM)**	**0**	*None*
6	~~**Cybersecurity Governance (CG)**~~		*None*
7	**ID & Authorization (IDA)**	**0**	*None*
8	**Incident Response (IR)**	**4**	**P1093** Detect & report events; **P1094** Analyze & triage events to support event resolution and incident declaration. **P1096** Develop and implement responses to declared incident according to predefined procedures; **P1097** Perform root cause analysis on incidents to determine underlying causes.
9	**Maintenance (MA)**	*None*	*None*
10	**Media Protection (MP)**	**0**	*None*
11	**Personnel Security (PS)**	**0**	*None*
12	**Physical Protection (PP)**	**0**	*None*
13	**Recovery (RE)**	**2**	**P1137** Regularly perform and tet data back-ups. **P1139** Regularly perform complete and comprhensive data back-ups and store them off-site and offline.
14	**Risk Management (RM)**	**3**	**P1144** Periodically perform **risk assessments** to identify and proitize risks according to the defined risk categories, risk sources, and risk measuement criteria; **P1146** Develop and implement **risk mitigation plans**; **P1147** Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.
15	**Security Assessment (SAS)**	**1**	**P1162** Employ **code reviews** of enterprise software developed for internal use to identify aneas of concern that require additional improvements.
16	**Situational Awareness (SA)**	**1**	**P1169** Receive and respond to **cyber threat intelligence** from information sharing forums and sources and communicate to stakeholders.
17	**System & Comms Protection (SCP)**	**3**	**P1179** Use encrupted sessions for the mnagement of network devices; **P1192** Implement Domain Name System (DNS) filtering services; **P1193** Implement a policy restricting the publication of CUI on publically accessible websites (e.g., Forums, LinkedIn, Facebook, Twitter, etc)
18	**System & Info. Integrity (SII)**	**3**	**P1218** Employ spam protection mechanisms at information system access entry and exit points. **P1219** Implement DNS or asymmetric cryptography email protections ; **P1220** Utilize email sandboxing to detect or block potentially malicious email attachments.
	TOTAL	**21**	

The additional practices in the Risk Assessment (RA) domain require that risk analyses be performed, risks prioritized, and a risk mitigation plan be put into place. Performing risk analysis (including analyses of threats, the impact of threats identified, and the likelihood of occurring) is a best practice in security designs of information systems. It is also the practice that will allow the system owners to uniquely identify the threat profile for their system, and in turn develop the security design for the system to mitigate threats and all risks.

Any code developed should be assessed to determine what risks may exist (domain Security Assessment (SAS). The additional practice in the Situational Awareness (SA) calls for obtaining a source of cyber intelligence from threat sharing forums.

Additional practices in the Systems and Communications Protection (SCP) require encrypted sessions during device maintenance, the implementation of DNS filtering services, and a policy restricting and controlling the publication of CUI data on publicly accessible websites including Facebook and other social media.

Finally, the new practices in the System and Information Integrity (SII) domain require spam protection mechanisms at the access and exit points of a network, the use of encryption to protect email, and the use of email sandboxing to detect and block malicious attachments.

COMPARISON TO OTHER STANDARDS

The original comparison of the complexity of CMMC v0.4 to other standards showed that the former CMMC level 3 had more practices, requirements and processes than the most complex and strong security baselines of FIPS Enhanced or CNSSI 1253 H-H-H baselines.

That picture has changed dramtically as shown in Figure 8. CMMC v0.6 level 3 with a total of 136 practices and processes is in the cluster of baselines including ISO 27001, FIPS L-L-L, CNSSI 1253 L-L-L and, of course , NIST 800-171. This is a good security baseline and profile, yet one that is achieveable.

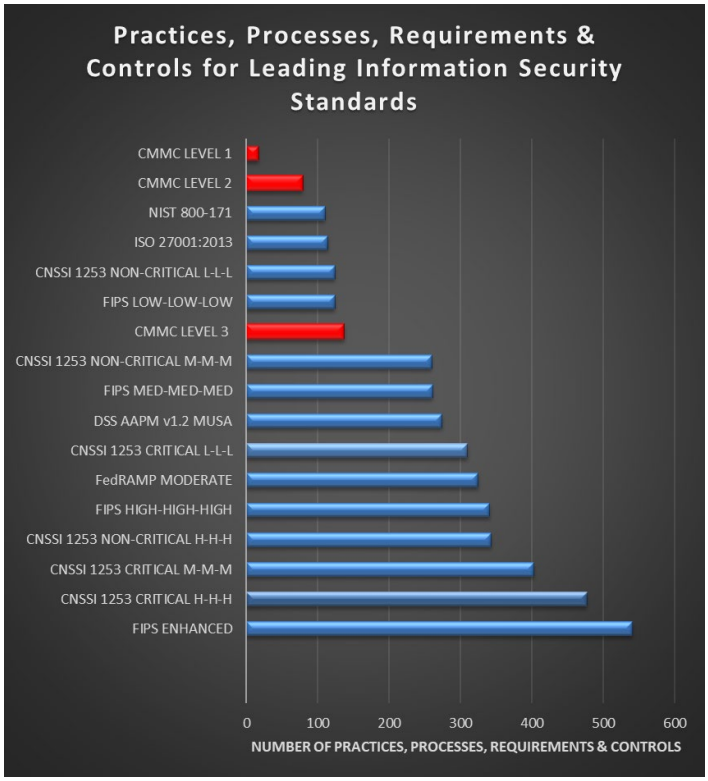

Figure 8 Comparison of CMMC to Other Security Frameworks &

SUMMARY

The CMMC v0.6 fulfills the OSD promise of NIST 800-171 at level 3 and FAR 52.204-21 at the lower levels. Levels 4 and 5 will include NIST 800-171B and other CMMC controls. The additional 21 practices bring significant value.

The unknown unknown still remains the definition of the work to be performed at each level of maturity. Consensus is that Level 3 will be the minimum level for any work that involvels sensitive data or CUI. CMMC makes reference to the AIA NAS 9933 standard, and AIA makes it clear that they require Level 3 for important work. The guidance provided in the DoD briefings indicate that level 3 will provide only "*moderate resistance against data exfiltration,"* and level 2 states that it provides only *"minor resistance to data exfiltration."* These definitions might be interpreted in a way that indicates level 4 is the first acceptable level. Without understanding the operational aspects of the CMMC, it is difficult to comment intelligently. DoD needs to clarify this information. Without a good definition and common understanding, the CMMC could be used as a procurement screen in a very arbitrary manner.

CMMC v0.6 is only a partial installment of the CMMC but, nonetheless, indicates significant change from the previous version and a return to the neighborhood of NIST 800-171.

Let us know what you think. Submit comments to https://nationalcyber.org/CMMC and the DIB ISAC, and the NCX will make sure all comments are received by the CMMC team.

References

1. Preliminary Analysis of CMMC v0.4, A Green Paper: Analysis of The DoD Cybersecurity Maturity Model Certification (CMMC) v0.6 Soliciting Input and Comments,M.G. Semmens, J. Kurtz, S. Lines, November, 2019.
2. *'Cybersecurity Maturity Model Certification (CMMC): Draft CMMC Model REV 064 Release & Request for Feedback',* Briefing, Office of the Undersecretary of Defense, Acquisition and Sustainment, U.S. Department of Defense, September 2019. https://www.acq.osd.mil/cmmc/docs/cmmc-overview-brief-30aug19.pdf
3. *Cybersecurity Maturity Model Certification (CMMC): Unclassified Draft Version 0.4,* Office of the Undersecretary of Defense, Acquisition and Sustainment, U.S. Department of Defense, Copyright 2019 Carnegie Mellon University and Johns Hopkins Applied Physics Laboratory, August 30, 2019. https://www.acq.osd.mil/cmmc/docs/cmmc-draft-model-30aug19.pdf

Acronyms

ACRONYM	DESCRIPTION
ACI	Additional Control Item
ACSC	Australian Cyber Security Centre
AIA	Aerospace Industries Association
APL	Johns Hopkins University Applied Physics Laboratory
CERT	Computer Emergency Response Team
CERT®	CERT™ / CERT® is a mark owned by Carnegie Mellon University
CERT®-RMM	CERT® Resilience Management Model
CIS	Center for Internet Security
CIS CSC	CIS Critical Security Controls
CMMC	Cybersecurity Maturity Model Certification (Copyright of Carnegie Mellon University and Johns Hopkins University)
CMMI	Capability Maturity Model Integration
CMMI®	CMMI® is a registered mark owned by Carnegie Mellon University
CMU	Carnegie Mellon University
CNSS	Committee on National Security Systems
CNSSI 1253	Committee on National Security Systems Instructions 1253 *"Security Categorization and Control Selection for National Security Systems"*
CSF	NIST Cybersecurity Framework
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DIB ISAC	Defense Industrial Base Information Sharing and Analysis Center
DNS	Domain Name Service
DoD	Department of Defense
DoD OIG	Department of Defense Office of the Inspector General
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standards
ISO	International Organization for Standardization
NAS	National Aerospace Standards
NCX	National Cyber Exchange
NIST	National Institute of Standards and Technology
NSS	National Security System
RCI	Referenced Control Item
RMF	Risk Management Framework
SEI	Software Engineering Institute of Carnegie Mellon University (an FFRDC)
SEI-CERT®	The CERT Division of the SEI
SME	Subject Matter Expert
UK NCSC	United Kingdom National Cyber Security Centre

Appendix A: NIST 800-171 Requirements v FAR 52.204-21 b.1

NIST 800-171		FAR Cyber Requirements
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
3.1.20	Verify and control/limit connections to and use of external systems.	(iii) Verify and control/limit connections to and use of external information systems.
3.1.22	Control CUI posted or processed on publicly accessible systems.	(iv) Control information posted or processed on publicly accessible information systems.
3.5.1	Identify system users, processes acting on behalf of users, and devices.	(v) Identify information system users, processes acting on behalf of users, or devices.
3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a pre-requisite to allowing access to organizational information systems.
3.8.3	Sanitize or destroy system media containing **CUI** before disposal or release for reuse.	(vii) Sanitize or destroy information system media containing **Federal Contract Information** before disposal or release for reuse.
3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
3.10.3	Escort visitors and monitor visitor activity.	(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
3.10.4	Maintain audit logs of physical access.	
3.10.5	Control and manage physical access devices.	
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational in-formation systems) at the external boundaries and key internal boundaries of the in-formation systems.
3.13.5	Implement subnetworks for publicly accessible system components that are	(xi) Implement subnetworks for publicly accessible system components that are

	physically or logically separated from internal networks.	physically or logically separated from internal networks.
3.14.1	Identify, report, and correct system flaws in a timely manner.	(xii) Identify, report, and correct information and information system flaws in a timely manner.
3.14.2	Provide protection from malicious code at designated locations within organizational systems.	(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
3.14.4	Update malicious code protection mechanisms when new releases are available.	(xiv) Update malicious code protection mechanisms when new releases are available.
3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.