HUB FOR CYBERSECURITY EDUCATION & AWARENESS HCEA

Cyber Law and Policy
Recent Updates

Joe Jabara, Col (Ret), JD

joe.jabara@wichita.edu

HUB FOR CYBERSECURITY EDUCATION & AWARENESS HCEA

HUB FOR CYBERSECURITY EDUCATION & AWARENESS HCEA

CMMC

- On Jan 30, DoD released Version 1.0 of the Cybersecurity Maturation Model
- 390 Pages
- Requires DoD Contractors to obtain certification later this year

HUB FOR CYBERSECURITY EDUCATION & AWARENESS HCEA

Why was this created?

- **Combat malicious cyber actors targeting intellectual property in the DoD's supply chain**
- **Ultimately will replace/combine other "pieced together" standards such as NIST SP 800-171 for DFARs and FARs**
- **Introduced a Level Based Compliance Structure for DoD Contractors**

HUB FOR CYBERSECURITY EDUCATION & AWARENESS HCEA

Level	Focus	Process Maturity	Practice Maturity
Level 1	Safeguard FCI	**Performed** No process assessment	**Basic Cyber Hygiene** 17 practices (meeting FAR Clause 52.204-21)
Level 2	Transition step to protecting CUI	**Documented** Document policies and implement practices	**Intermediate Cyber Hygiene** 72 practices
Level 3	Protect CUI	**Managed** Establish, maintain and resource a plan	**Good Cyber Hygiene** 130 practices (includes all NIST SP 800-171 plus others)
Level 4	Protect CUI and reduce risk of advanced persistent threats	**Reviewed** Review and measure activities for effectiveness	**Proactive** 156 Practices
Level 5		**Optimizing** Standardize and optimize an organizational approach	**Advanced/Progressive** 171 Practices

HUB FOR CYBERSECURITY EDUCATION & AWARENESS HCEA

Graded Areas

- **Basic: Access Control, Audit and Accountability, Incident Response, Risk Management, Systems and Communications Protection, and System and Information Integrity**
- **Advanced: See Chart**
- **Introduced a Level Based Compliance Structure for DoD Contractors**

HUB FOR CYBERSECURITY EDUCATION & AWARENESS HCEA

Table 1. CMMC Capabilities

Domain	Capability
Access Control (AC)	• Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes
Asset Management (AM)	• Identify and document assets
Audit and Accountability (AU)	• Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs
Awareness and Training (AT)	• Conduct security awareness activities • Conduct training
Configuration Management (CM)	• Establish configuration baselines • Perform configuration and change management
Identification and Authentication (IA)	• Grant access to authenticated entities
Incident Response (IR)	• Plan incident response • Detect and report events • Develop and implement a response to a declared incident • Perform post incident reviews • Test incident response
Maintenance (MA)	• Manage maintenance
Media Protection (MP)	• Identify and mark media • Protect and control media • Sanitize media • Protect media during transport
Personnel Security (PS)	• Screen personnel • Protect CUI during personnel actions
Physical Protection (PE)	• Limit physical access
Recovery (RE)	• Manage back-ups
Risk Management (RM)	• Identify and evaluate risk • Manage risk
Security Assessment (CA)	• Develop and manage a system security plan • Define and manage controls • Perform code reviews
Situational Awareness (SA)	• Implement threat monitoring
Systems and Communications Protection (SC)	• Define security requirements for systems and communications • Control communications at system boundaries
System and Information Integrity (SI)	• Identify and manage information system flaws • Identify malicious content • Perform network and system monitoring • Implement advanced email protections

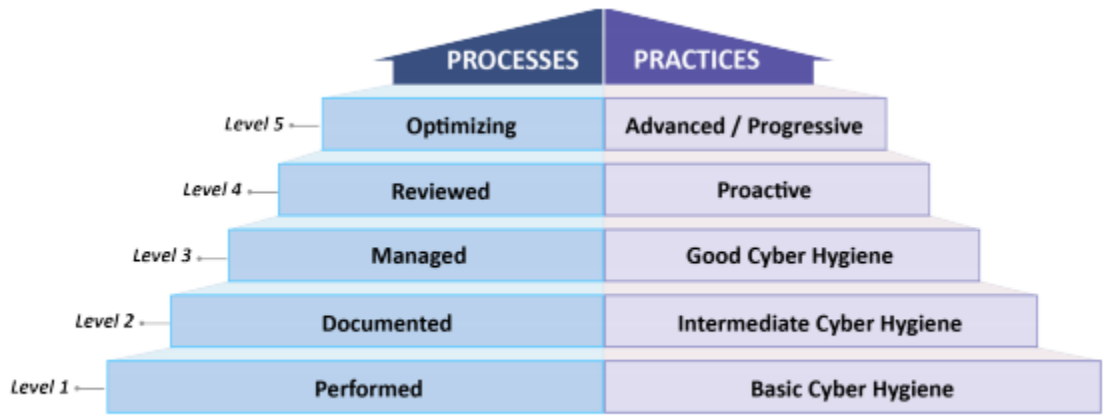

Figure 2. CMMC Levels and Descriptions

HUB FOR CYBERSECURITY EDUCATION & AWARENESS HCEA

Other Key Highlights

- Independent 3rd party assessment organization will normally perform the assessment.
- Some higher level assessments may be performed by organic DoD assessors within the Services, the Defense Contract Management Agency (DCMA) or the Defense Counterintelligence and Security Agency (DCSA).
- Certification level will be made public
- All companies conducting business within DoD need to be certified

HUB FOR CYBERSECURITY EDUCATION & AWARENESS HCEA

Legal Ramifications

- Will not be awarded Government Contracts if shown as Non Compliant
- Should self inspections/pre audit activity be held under attorney/client work product privilege?
- Whistleblower Cases
- These are also industry standards….if not followed breach could occur and legal liability could ensue (see WaWa Case as example)

HUB FOR
CYBERSECURITY
EDUCATION & AWARENESS
HCEA

HUB FOR
CYBERSECURITY
EDUCATION & AWARENESS
HCEA

The emerging nature of cyber risk is that it's becoming systemic - as were the risks that led to the credit crisis.

John Scott
Chief Risk Officer
Global Corporate, Zurich - June 2015

HUB FOR CYBERSECURITY EDUCATION & AWARENESS HCEA

Federal Legislation on the Table

House-passed cybersecurity legislation

R. 3710 - Cybersecurity Vulnerability Remediation Act: This bill was passed by the House in September and is now before the Senate Homeland Security and Governmental Affairs Committee, which has taken no action yet. The bill would allow the Department of Homeland Security's (DHS's) Cybersecurity and Infrastructure Security Agency (CISA) to issue protocols to mitigate vulnerabilities, and would allow the Science and Technology Directorate of the Department of Homeland Security to establish an incentive program that allows industry, individuals, academia, and others to compete in providing remediation solutions for cybersecurity vulnerabilities.

R.2331 - SBA Cyber Awareness Act and H.R.1649 - Small Business Development Center Cyber Training Act of 2019: Both bills passed the House on July 15. The SBA Cyber Awareness Act addresses the cybersecurity of the Small Business Administration (SBA). It requires the SBA to report annually to Congress on SBA's IT technology and any necessary improvements the agency's technology infrastructure may need. It also requires SBA to provide an account of its IT equipment or interconnected system or subsystem of equipment manufactured by an entity that has its principal place of business in the People's Republic of China.

The annual report must further provide accounts of any cybersecurity incident SBA has encountered during the previous two years and how the government agency dealt with the incidents. The Small Business Development Center Cyber Training Act requires the SBA to establish a program for certifying that at least 5% or 10% of the total number of employees of a small business development center provide cybersecurity planning assistance to small businesses. Both bills have companion legislation in the Senate sponsored by Sen. Marco Rubio (R-FL) who chairs the Senate Small Business Committee and are awaiting votes by the full Senate.

R. 328 - Hack Your State Department Act: This bill was one of the first cybersecurity measures passed by the House during the 116th Congress, enacted last January and quickly referred to the Senate where companion legislation was introduced on June 12. It requires the "Secretary of State to design and establish a Vulnerability Disclosure Process (VDP) to improve Department of State cybersecurity" and mandates a bug bounty program "to identify and report vulnerabilities of internet-facing information technology of the Department of State."

R. 1 - For the People Act of 2019: The first bill introduced in the new Congress was passed by the House on March 8. Among other things, this sweeping piece of legislation "sets forth provisions related to election security, including sharing intelligence information with state election officials, protecting the security of the voter rolls, supporting states in securing their election systems, developing a national strategy to protect the security and integrity of U.S. democratic institutions, establishing in the legislative branch the National Commission to Protect United States Democratic Institutions."

Senate-passed

1. 333 - National Cybersecurity Preparedness Consortium Act of 2019: Passed by the Senate on November 21 and referred to the House Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation on December 4, the bill allows the Department of Homeland Security to work together with a consortium composed of nonprofit entities to develop, update, and deliver cybersecurity training in support of homeland security.

2. 1846 - State and Local Government Cybersecurity Act of 2019: Passed by the Senate on November 21 and referred to the House Committee on Homeland Security, and the Committees on Oversight and Reform, and Energy and Commerce on November 26, the bill authorizes the Homeland Security secretary to make grants to and enter into cooperative agreements or contracts with states, local, tribal, and territorial governments, and other non-federal entities, that the secretary determines necessary regarding cyber threat indicators, defensive measures and cybersecurity technologies, cybersecurity risks, incidents, analysis, and warnings.

3. 406 - Federal Rotational Cyber Workforce Program Act of 2019: Passed by the Senate on April 30, 2019 and considered by the House Committee on Oversight and Reform, which has already held one markup session, the bill permits certain government agency employees to detail among rotational cyber workforce positions at other agencies.

Cybersecurity legislation in committee

A number of bills have been introduced or moved in either House or Senate committees and are likely candidates for further movement once Congress rolls up its sleeves after recess ends. Among them are:

1. R. 3941 - The Federal Risk Authorization and Management Program (FedRAMP) Authorization Act: Introduced by the House on July 24, 2019 with the House Oversight and Reform Committee holding a markup session on December 19, 2019, this legislation is now ready for full House consideration. The bill establishes the Federal Risk and Authorization Management Program (FedRAMP) within the General Services Administration. FedRAMP is a risk management, authorization, and continuous monitoring process to enable the Federal Government to leverage cloud computing services using a risk-based approach consistent with the Federal Information Security Modernization Act of 2014 and cloud-based operations. It also allocates $20 million for the initiative.

2. R.1668 - IoT Cybersecurity Improvement Act of 2019: Introduced on March 11, 2019, the bill was approved by the House Committee on Oversight and Reform and is awaiting action by the Committee on Science, Space, and Technology. On the Senate side, the companion bill (S.734) has been approved by the Homeland Security and Governmental Affairs Committee and is sitting on the Senate legislative calendar. The bill would give the National Institute of Standards and Technology (NIST) the authority for managing internet-of-things (IoT) cybersecurity risks for devices acquired by the federal government.

3. R.4237 - Advancing Cybersecurity Diagnostics and Mitigation Act: Introduced in the House on September 6, 2019 and passed by the Committee on Homeland Security in October, the bill is awaiting consideration by the House Oversight and Reform Committee. The legislation's Senate Companion (S. 2318) has yet to be considered or amended by the Homeland Security and Governmental Affairs Committee. The bill authorizes the Secretary of Homeland Security to establish a continuous diagnostics and mitigation program in the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security..

4. 3033 - K-12 Cybersecurity Act of 2019: This bill was introduced in the Senate Homeland Security and Government Affairs Committee shortly before recess on December 12, 2019 and is a response to the rash of ransomware attacks on government institutions and schools during 2019. It calls for DHS to create a set of guidelines to help schools improve their cybersecurity posture to better ward off these attacks.

Hot cybersecurity topics

Aside from the formal measures introduced in or passed by the House or Senate, a number of hot topic cybersecurity issues are emerging as key subject areas for new legislation or at least high-level Congressional debate during 2020.

1. Election security: Despite an additional $425 million authorized by Congress to strengthen election security at the state level as part of appropriations bills passed in December, Democrats believe Congress hasn't done enough to protect the country while the presidential election year moves into full swing. Senator Ron Johnson (R-WI), Chairman of the Senate Homeland Security and Governmental Affairs Committee, said he plans to hold hearings on the topic in 2020. House Administration Committee Chairwoman Zoe Lofgren might hold oversight hearings on the topic early in the year.

2. Ransomware threats: 2019 saw a rash of ransomware attacks that crippled the city governments of Baltimore, Pensacola and New Orleans along with a number of other municipalities in the U.S. Although two bills have been introduced to help local governments deal with this growing concern, the State and Local Government Cybersecurity Act of 2019 and the K-12 Cybersecurity Act of 2019, it's likely that lawmakers will focus additional attention on these threats, particularly if more high-profile government ransomware attacks occur.

3. Foreign apps: As fears of supply chain threats ramp up in the U.S., with notable bans implemented by the Trump Administration on Chinese tech companies such as Huawei, a new avenue of concern has opened up regarding popular consumer apps that originate outside the U.S. The U.S. Navy and Army have already banned their personnel from using Chinese viral video app TikTok on government issued phones. New reports indicate that popular Middle Eastern app ToTok is being used as spyware for the government of the United Arab Emirates, sparking some lawmakers to express concern over the national security implications of the app.

4. DHS subpoena power: The DHS has floated a legislative proposal to give it subpoena power to speed up CISA's ability to interact with critical infrastructure companies that are the targets of foreign cyberattacks. The administrative subpoena power that DHS seeks would require ISPs to turn over information on equipment owners for which CISA has IP addresses so that the agency can contact them about the threats.

Another development worth watching as Congress returns from recess is the emergence of a federal strategy for defending the U.S. government against cyberattacks that lawmakers say could be finalized as early as March. The strategy flows from a commission created after the passage of the 2018 National Defense Authorization Act and a draft version of the commission's report is already circulating among lawmakers. The report will focus on protecting federal assets from cyberattacks but could prove useful to state and local government, too.


© Jon Carter • cartertoons.com
WHAT HAPPENED TO THE GOOD OLD DAYS WHEN PEOPLE JUST BREACHED CONTRACTS?
BREAKING NEWS
ANOTHER DATA BREACH

Privacy

- General Data Protection Regulation (GDPR)-EU Based
  - What types of privacy data does the GDPR protect?
    - Basic identity information such as name, address and ID numbers
    - Web data such as location, IP address, cookie data and RFID tags
    - Health and genetic data
    - Biometric data
    - Racial or ethnic data
    - Political opinions
    - Sexual orientation
  - Applies to any company that stores or processes personal information about EU citizens within EU states must comply with the GDPR, even if they do not have a business presence within the EU.
  - The GDPR places equal liability on data controllers (the organization that owns the data) and data processors (outside organizations that help manage that data)
  - 72 Hours to Report a Breach

Privacy

- California Consumer Privacy Act
  - Allows any California consumer to demand to see all the information a company has saved on them, as well as a full list of all the third parties that data is shared with.
  - California law allows consumers to sue companies if the privacy guidelines are violated, even if there is no breach.
  - All companies that serve California residents and have at least $25 million in annual revenue or stores data on 50,000 people and gets 50% of revenue from data storage must comply with the law.
  - Companies don't have to be based in California or have a physical presence there to fall under the law. They don't even have to be based in the United States.
  - Effective 1 January 2020

Privacy

- HIPAA-Due for Rewrite
- Sarbanes-Oxley-Under Review
- New York, Florida, Others Jumping on CCPA Model

Equifax

Case Trends

- Negligence for Failing to Meet Industry Standards in Security Practices
- Privacy Notices-Implied Contracts
- Failure to Notify of Breach
- Tort Invasion of Privacy
- Hacker rarely gets sued

Dunkin Donuts Lawsuit

HUB FOR CYBERSECURITY EDUCATION & AWARENESS HCEA

Questions????

One Last Bit of Advice