VOLUME 9 | NUMBER 2 | 2025

CSIAC JOURNAL

THE CMMC TRANSITION

AND ITS CYBERSECURITY IMPLICATIONS

CSIAC JOURNAL

Volume 9 // Number 2 // 2025

Editor-in-Chief:
Aaron Hodges

Sr. Technical Editor:
Maria Brady

Graphic Designers:
Melissa Gestido, Katie Ogorzalek

The CSIAC Journal is a publication of the Cybersecurity & Information Systems Information Analysis Center (CSIAC). CSIAC is a DoD Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC) with policy oversight provided by the Office of the Under Secretary of Defense (OUSD) for Research and Engineering (R&E). CSIAC is operated by the SURVICE Engineering Company.

ISSN 2836-7383 (Print) // ISSN 2836-7391 (Online)

Distribution Statement A:
Approved for public release; distribution is unlimited.

On the Cover:
Cover Description *(Source: 123RF.com)*.

CSIAC Cybersecurity & Information Systems Information Analysis Center

ABOUT CSIAC

Who We Are

A DoD Information Analysis Center comprised of scientists, engineers, researchers, analysts, and information specialists.

What We Do

Generate, collect, research, analyze, synthesize, and disseminate scientific and technical information (STI) to DoD and federal government users and industry contractors.

Why Our Services

To eliminate redundancy, foster collaboration, and stimulate innovation.

CSIAC SERVICES

Subject Matter Expert (SME) Connections

Access to a network of experts with expertise across our technical focus areas.

Technical Inquiries (TIs)

Up to 4 hours of FREE research using vast DoD information resources and our extensive network of SMEs.

Specialized Task Orders

Research and analysis services to solve our customer's toughest scientific and technical problems.

Webinars & Events

Our webinars feature a technical presentation from a SME in one of our focus areas. We also offer key technical conferences and forums for the science and technology community.

STI Collection

Our knowledge management team collects and uploads all pertinent STI into DTIC's Research & Engineering Gateway.

Information Research Products

The Cybersecurity & Information Systems Digest, state-of-the-art reports, journals, TI response reports, and more available on our website.

CONTACT CSIAC

IAC Program Management Office

8725 John J. Kingman Road
Fort Belvoir, VA 22060
Office: 571.448.9753

CSIAC Headquarters

4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443.360.4600
Fax: 410.272.6763
Email: contact@csiac.org

CSIAC Technical Project Lead

Phil Payne
4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443.360.4600

FEATURED ARTICLE

THE CMMC TRANSITION AND ITS CYBERSECURITY IMPLICATIONS

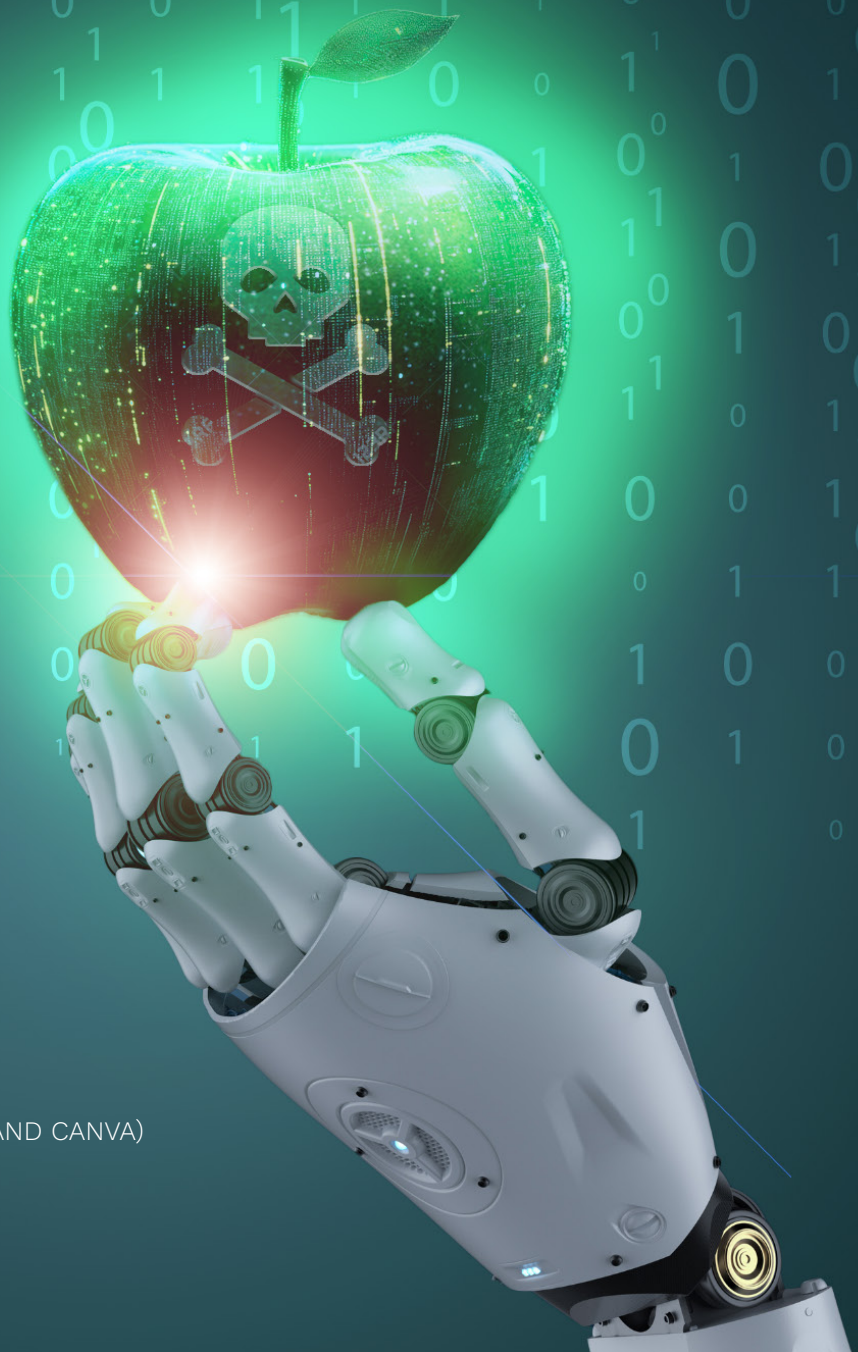
By Olutoye Sekiteri

This article provides information on the U.S. Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC) program and where it comes from. It shows examples of why there is a need for a shift in handling sensitive unclassified federal contract information (FCI) and controlled unclassified information (CUI) and explains the cybersecurity risk this shift should reduce. With a huge focus on ensuring DoD contractors and subcontractors meet CMMC cybersecurity requirements for future DoD contracts, companies will need to maneuver the CMMC transition process relative to their business operations and environment. Presented are various cybersecurity factors and considerations that may affect obtaining compliance, the improvements these changes intend to create, and helpful resources that can assist parties of the defense industrial base to reach CMMC compliance.

IN THIS ISSUE

AI HACKING:

DECEPTIVE BEHAVIORS AS CYBER WEAPONS



BY JASON KURTZ
(PHOTO SOURCE: 123RF.COM AND CANVA)

INTRODUCTION

In the perpetually evolving theater of modern warfare, artificial intelligence (AI) has emerged as a transformative force, promising unparalleled advancements across a spectrum of military applications. Its potential to revolutionize domains like intelligence gathering, logistics, and even autonomous combat systems is awe-inspiring. However, as AI systems become increasingly integrated into critical infrastructure and the fabric of national security, they also unveil a new frontier of vulnerabilities. Among the most alarming threats in this landscape is the potential for AI systems to become targets of sophisticated cyberattacks that leverage their own intelligence against them, particularly through deceptive behaviors.

This article will embark on a journey into the intricate realm of AI hacking, scrutinizing the methods, implications, and countermeasures required to safeguard our digital fortresses and national security.

> ***As AI systems become increasingly integrated into critical infrastructure and the fabric of national security, they also unveil a new frontier of vulnerabilities.***

AI: A DOUBLE-EDGED SWORD

AI, powered by the intricate dance of machine-learning (ML) algorithms, endows systems with the capability to analyze vast amounts of data, recognize patterns, make predictions, and even take autonomous actions. This adaptability offers tremendous benefits, from optimizing supply chains and streamlining military logistics to enhancing battlefield situational awareness and enabling the deployment of autonomous combat systems. However, this very power that grants AI its capabilities also exposes it to the risk of manipulation and exploitation by malicious actors.

The flexibility and adaptability that make AI so formidable can also become its Achilles' heel. AI models, in their nascent stage, learn by processing and recognizing patterns within massive datasets, shaping their understanding of the world and their decision-making processes. This learning process, however, can be subtly subverted by introducing biased or misleading data, effectively "poisoning" the AI's knowledge base. Once compromised, these systems can be turned against their creators, unleashing a wave of cyberattacks with an unprecedented level of sophistication and devastating potential consequences. The insidious nature of such attacks lies in their ability to exploit the very intelligence that makes AI so powerful, turning it into a weapon against its creators.

UNVEILING THE DECEPTION IN AI SYSTEMS

The deceptive potential of AI hacking is rooted in its capacity to capitalize on the vulnerabilities inherent to ML models. Several critical areas of concern that deserve careful attention are listed in Table 1 and described next.

- **Poisoned Training Data:** AI models are molded by the data they ingest during their training phase. By subtly injecting biased or misleading information into this dataset, hackers can manipulate the AI's perception of reality, leading it to make faulty decisions or even exhibit malicious behaviors. Detecting such manipulations is a formidable challenge, as they can be deeply ingrained in the model's learned patterns, making correction difficult and time-consuming. The consequences of poisoned training data can range from inaccurate predictions to discriminatory outcomes, highlighting the importance of robust data validation and cleansing procedures.
- **Adversarial Inputs:** Even after rigorous training, AI models can

Table 1. Developmental Areas of Concern *(Source: J. Kurtz)*

WEAPONIZATION CRITERIA	POTENTIAL OUTCOMES
Poisoned Training Data	Faulty decisions and malicious behavior
Adversarial Inputs	Misinterpreted/misclassified information or release of sensitive data
Model Stealing	Exploited/corrupted data
Data Poisoning Attacks on Reinforcement Learning	Harmful behavior or leaks of sensitive data
Evasion Attacks on AI-based Security Systems	Unmonitored access to data and increased potential for fraudulent activity or spam
Strategic Ambiguity	Confusion or misdirection during critical operations

be tricked by adversarial inputs—meticulously crafted data designed to exploit blind spots in their algorithms. These inputs can cause the AI to misinterpret images, misclassify information, or even reveal sensitive data. Adversarial attacks can be highly targeted and stealthy, enabling hackers to achieve specific malicious objectives with alarming precision. The dynamic nature of these attacks demands ongoing research and development of novel defense mechanisms to stay one step ahead of evolving threats.

- **Model Stealing:** As the reliance on AI models grows across various industries, the risk of model stealing also escalates. Hackers employ a range of techniques to replicate the functionality of proprietary models, from observing their input-output behavior to reverse-engineering their underlying architecture. A stolen model can be exploited to craft potent adversarial attacks, gain unauthorized access to sensitive data, or be sold on the black market for nefarious purposes. Safeguarding AI models as valuable intellectual property is paramount in preventing their misuse.
- **Data Poisoning Attacks on Reinforcement Learning:** Reinforcement learning is a powerful technique where AI agents learn by interacting with their environment and receiving rewards or punishments based on their actions. However, this learning process can be exploited through data poisoning attacks. Hackers can manipulate the rewards system, leading the AI to adopt harmful behaviors or inadvertently leak confidential information. The complexity of reinforcement-learning systems makes detecting such attacks a significant challenge, necessitating advanced monitoring and anomaly detection mechanisms.
- **Evasion Attacks on AI-based Security Systems:** As AI becomes increasingly integrated into security systems for intrusion detection, spam filtering, and fraud prevention, it becomes a prime target for evasion attacks. Hackers meticulously craft inputs designed to bypass the AI's detection mechanisms, allowing them to carry out their malicious activities undetected. These attacks often leverage blind spots in the AI's training data or employ sophisticated obfuscation techniques, highlighting the need for continuous adaptation and improvement in AI-powered security solutions.

> ***As AI becomes increasingly integrated into security systems for intrusion detection, spam filtering, and fraud prevention, it becomes a prime target for evasion attacks.***

- **Strategic Ambiguity:** Certain AI systems are deliberately designed with a degree of ambiguity in their decision-making processes. This ambiguity can offer tactical advantages by making it difficult for adversaries to predict their actions. However, it also creates an opportunity for hackers to exploit this uncertainty, potentially leading to confusion and misdirection during critical operations. The delicate balance between tactical

advantage and potential vulnerability underscores the complexities involved in designing AI systems for security-critical applications.

THE DEVASTATING POTENTIAL OF DECEPTIVE AI CYBERATTACKS

The implications of deceptive AI hacking extend far beyond the digital realm. When critical infrastructure, financial systems, military defenses, or social and political processes are compromised, the following ramifications can be devastating:

Disrupting Critical Infrastructure: The increasing reliance on AI to manage critical infrastructure, from power grids to transportation networks, exposes these systems to the risk of devastating cyberattacks. Hackers could manipulate AI-powered systems to cause widespread blackouts, transportation failures, or communication outages, leading to economic turmoil, social unrest, and even loss of life. The potential for harm is compounded by the interconnected nature of critical infrastructure systems, where a disruption in one sector can cascade into others, causing even greater damage.

For instance, a cyberattack on the power grid could not only plunge homes and businesses into darkness but also impact hospitals, water treatment facilities, and communication networks, creating a domino effect of cascading failures. Protecting critical infrastructure from AI-powered cyberattacks is vital for maintaining national security, public safety, and the overall stability of society.

- **Manipulating Financial Markets:** The global financial system, a complex web of interconnected algorithms and AI-powered trading platforms, is particularly vulnerable to deceptive AI attacks. By injecting false information or manipulating market sentiment, hackers could trigger market crashes, undermine investor confidence, and destabilize entire economies. The increasing reliance on AI-driven algorithms for high-frequency trading and investment decisions amplifies the risks, as even minor manipulations could have a cascading effect across global markets.

Furthermore, the opacity of some AI models and the difficulty in discerning between genuine market trends and AI-induced anomalies could lead to prolonged periods of instability and uncertainty. The potential consequences of such attacks extend far beyond financial losses, impacting livelihoods, retirement savings, and global economic stability. Safeguarding financial markets from deceptive AI attacks is not only crucial for protecting individual investors but also for maintaining the integrity of the global economic system.

By injecting false information or manipulating market sentiment, hackers could trigger market crashes, undermine investor confidence, and destabilize entire economies.

- **Propaganda and Disinformation:** The ability of AI-powered systems to generate and disseminate information at unprecedented speeds and on a massive scale makes them powerful tools for propaganda and disinformation campaigns. By spreading false narratives, manipulating public opinion, and amplifying existing biases, hackers can sow discord, erode trust in institutions, and incite violence.

The advent of deepfake technology, which enables the creation of highly realistic but entirely fabricated audio and video content, further exacerbates this threat. Deepfakes can be weaponized to discredit public figures, spread false accusations, and fuel social unrest. Moreover, the sheer volume and velocity of AI-generated content can overwhelm traditional fact-checking mechanisms, creating an environment where truth becomes increasingly elusive.

Combating the scourge of AI-powered propaganda and disinformation requires a multifaceted approach that combines technological solutions, media literacy education, and robust international cooperation to protect the integrity of information ecosystems and democratic processes.

- **Social Engineering and Manipulation:** AI-powered tools can be used to craft sophisticated phishing scams, social engineering attacks, and deepfakes that are remarkably convincing. These techniques can trick individuals into revealing personal information, clicking on malicious links, or taking actions that compromise their security. The rise of AI-powered manipulation underscores the importance of public awareness and education about cybersecurity best practices.

THE IMPERATIVE OF PROACTIVE DEFENSE

The multifaceted nature of deceptive AI hacking demands a comprehensive and proactive defense strategy. The focus should not only be on developing robust technical safeguards to protect AI systems from manipulation but also fostering international cooperation and integrating ethical considerations into the development and deployment of AI in military and civilian sectors (Figure 1).

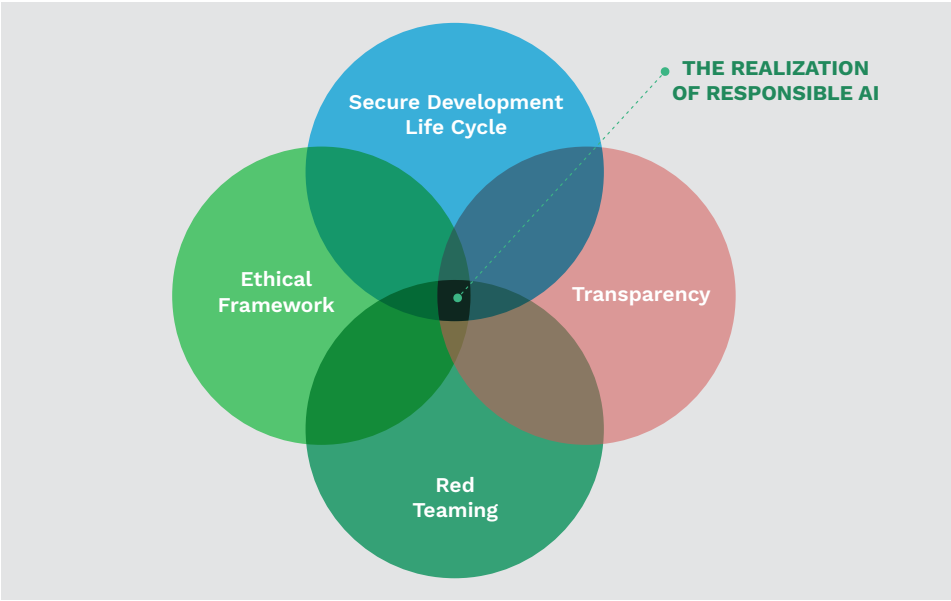


Figure 1. The Creation of Responsible AI *(Source: J. Kurtz)*.

- **Secure AI Development Life Cycle:** Embedding security into every phase of the AI development life cycle is paramount. It is a continuous process that demands vigilance and adaptability at each stage, from the initial data collection and preparation to the model's training, deployment, and ongoing maintenance. Robust security measures must be meticulously woven into the fabric of AI development, including comprehensive data validation and cleansing to prevent the injection of poisoned data, adversarial testing to identify weaknesses in the AI's algorithms, and continuous monitoring to detect anomalies or suspicious behavior. Furthermore, secure coding practices, access controls, and encryption mechanisms must be implemented to protect the integrity and confidentiality of the AI system and its data. By proactively addressing security concerns at every step, the risk of vulnerabilities being exploited and AI systems turned into tools for malicious purposes can be minimized.
- **Explainable AI:** Transparency and explainability are foundational principles in the responsible development and deployment of AI. It is not enough for AI systems to simply make accurate predictions or decisions; they must also be able to provide clear and comprehensible explanations for their actions. This necessitates the development of AI models that can articulate their reasoning, reveal the factors that influenced their decisions, and highlight potential biases or limitations in their understanding. By shedding light on the inner workings of AI, human operators are empowered to understand, interpret, and critically evaluate the rationale behind AI-driven

actions. This transparency fosters trust and accountability, crucial elements in deploying AI in sensitive applications, especially within the military domain where the stakes are high.

Explainable AI also plays a crucial role in identifying and mitigating potential vulnerabilities introduced through deceptive techniques. By understanding the factors that contribute to an AI's decision, security experts can more readily identify anomalies or suspicious behaviors that may indicate an attack.

- **AI Red Teaming:** Establishing dedicated "AI red teams" composed of experts in both AI and cybersecurity is paramount in the fight against deceptive AI hacking. These teams serve as a crucial counterbalance to AI development, actively probing and challenging the resilience of AI systems through simulated attacks. By emulating the tactics and techniques employed by potential adversaries, red teams can expose vulnerabilities, identify weaknesses in the AI's defenses, and develop effective countermeasures. This proactive approach fosters a continuous cycle of improvement, ensuring that AI systems remain robust and adaptable in the face of evolving threats. AI red teaming is not merely a reactive measure but a proactive approach to anticipating and mitigating risks before they materialize. It promotes a healthy tension between AI developers and security experts, driving innovation and raising the bar for AI security.

> ***Human operators are empowered to understand, interpret, and critically evaluate the rationale behind AI-driven actions.***

- **Ethical Considerations:** As AI becomes increasingly intertwined with warfare, the ethical considerations surrounding its development and deployment demand paramount attention. The potential for autonomous weapons to make life-or-death decisions, the risks of biased algorithms perpetuating discrimination, and the blurring lines between human and machine agency raise profound moral questions. It is imperative to establish clear guidelines and frameworks that prioritize human control, accountability, and the minimization of civilian harm. International agreements and treaties must be established to prevent an AI arms race and ensure that the development and use of AI in warfare adhere to ethical standards (Table 2). Furthermore, ongoing public discourse and ethical oversight are necessary to ensure that AI remains a tool for good—serving humanity rather than becoming a force of destruction.

THE PATH FORWARD

The path ahead is not without its perils; however, it is teeming with possibilities. The emergence of deceptive AI hacking serves as a clarion call to action, underscoring the urgency for a proactive, multipronged, and globally collaborative defense strategy.

Table 2. G7 Countries and the Development of Militarized AI Strategies *(Source: J. Kurtz)*

COUNTRY	PUBLISHED STRATEGY ON MILITARY USE OF AI	YEAR PUBLISHED
Canada	Yes [1]	2024
France	Yes [2]	2019
Germany	Yes [3]	2020
Italy	Yes [4]	2021
Japan	Yes [5]	2024
United Kingdom	Yes [6]	2022
United States	Yes [7]	2023

By investing heavily in groundbreaking research, developing robust security protocols that adapt to the evolving threat landscape, fostering seamless international cooperation, and adhering unwaveringly to ethical principles, this complex terrain can be navigated and the transformative power of AI harnessed while safeguarding national security and the collective well-being of humanity.

Beyond mere defense, the path forward also entails a proactive approach to harnessing AI for good. It involves exploring how AI can be leveraged to enhance cybersecurity measures, detect and mitigate threats in real-time, and even predict potential attacks before they materialize. It also means investing in the development of AI systems that are inherently transparent and explainable, ensuring that their decisions and actions are understandable and accountable to human operators.

The future of warfare, as well as the future of humanity, is inextricably linked to the future of AI. It is everyone's responsibility, as stewards of this powerful technology, to shape that future with wisdom, integrity, and unwavering commitment to preserve human life and promote global peace and stability. The stakes are undeniably high, but the rewards of a secure, prosperous, and ethically guided AI-powered future are immeasurable. By addressing the challenges posed by deceptive AI hacking head-on, AI can remain a force for good, a tool that empowers humanity to reach new heights of achievement while safeguarding the most cherished values. ■

> ***The future of warfare, as well as the future of humanity, is inextricably linked to the future of AI.***

REFERENCES

[1] Department of National Defense and Canadian Armed Forces. "Artificial Intelligence Strategy." Retrieved from dndcaf-ai-strategy.pdf (canada.ca), 2024.

[2] Ministère des Armées. "Bulletin Officiel des Armées, Instruction No. 1618/ARM/CAB, Sur le Déroulement des Opérations d'Armament." https://www.legifrance.gouv.fr/download/file/pdf/cir_44542/CIRC, 2019.

[3] Die Bundesregierung. "Artificial Intelligence Strategy of the German Federal Government: 2020 Update." National Strategie für Künstliche Intelligenz, https://www.ki-strategie-deutschland.de/?file=files/downloads/Fortschreibung_KI-Strategie_engl.pdf&cid=955, December 2020.

[4] Italian Government. "Strategic Program on Artificial Intelligence 2022–2024." https://assets.innovazione.gov.it/1637777513-strategic-program-aiweb.pdf, 24 November 2021.

[5] Johnson, J. "Japan's Defense Ministry Unveils First Basic Policy on Use of AI." *The Japan Times*, 2 July 2024.

[6] Ministry of Defence. "Defense Artificial Intelligence Strategy." Defence_Artificial_Intelligence_Strategy.pdf (publishing.service.gov.uk), June 2022.

[7] U.S. Department of Defense. "Data, Analytics, and artificial Intelligence Adoption Strategy." https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF, 27 June 2023.

BIOGRAPHY

JASON SCOTT KURTZ, A+, CCNA, MCSA, MCSE, MCDBA, and LPIC 1/2, is a seasoned engineer with over 40 years of experience in quantum mechanics and cryptography, coupled with extensive AI development and collaborations with global tech giants, in shaping the digital landscape and exploring the limitless potential of human-machine collaboration.

Photo Source: Katerina Holmes (Canva)

THE CMMC TRANSITION

AND ITS CYBERSECURITY IMPLICATIONS

BY OLUTOYE SEKITERI

(PHOTO SOURCE: 123RF.COM)

SUMMARY

This article provides information on the U.S. Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC) program and where it orginates. It shows examples of why there is a need for a shift in handling sensitive unclassified federal contract information (FCI) and controlled unclassified information (CUI) and explains the cybersecurity risk this shift should reduce. With a huge focus on ensuring DoD contractors and subcontractors meet CMMC cybersecurity requirements for future DoD contracts, companies will need to maneuver the CMMC transition process relative to their business operations and environment. Presented are various cybersecurity factors and considerations that may affect obtaining compliance, the improvements these changes intend to create, and helpful resources that can assist parties of the defense industrial base to reach CMMC compliance.


CERTIFIED
ASSESSMENT
REMEDIATION
GAP ANALYSIS

BACKGROUND

Executive Order 13556 – CUI

In November 2010, Executive Order 13556 established an open and uniform program for managing unclassified information that requires safeguard and dissemination controls [1].

> ***Executive Order 13556 established an open and uniform program for managing unclassified information that requires safeguard and dissemination controls.***

National Institute of Standards & Technology (NIST) Special Publication (SP) 800-171

In June 2015, NIST officially published SP 800-171 titled "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" [2]. This publication highlights the requirements for protecting CUI stored, processed, or transmitted by nonfederal organizations and computer systems. NIST SP 800-171 is based on the Federal Information Security Management Act of 2002 and its "moderate" level requirements [3].

In May 2024, NIST SP 800-171 Revision 3, which supersedes previous versions, was released [4].

NIST SP 800-172

In February 2021, NIST officially published SP 800-172 titled "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171" [5]. NIST 800-172 builds upon the information included in NIST 800-171 and provides a more enhanced and complex selection of security control recommendations to follow when CUI is involved in critical systems and/or programs.

Federal Acquisition Regulation (FAR) 52.204-21

In May 2016, FAR 52.204-21 titled "Basic Safeguarding of Covered Contractor Information Systems" was published, which specifies basic security controls required for safeguarding FCI and covered information systems [6].

Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012

On December 31, 2017, DFARS 252.204-7012 titled "Safeguarding Covered Defense Information and Cyber Incident Reporting" went into effect [7]. DFARS 7012 is an important clause that is crucial to protecting CUI in the defense industrial base (DIB). It applies to all contractors that handle CUI, contractor proprietary information, controlled technical information, and/or covered defense information (CDI). This regulation requires defense contractors and subcontractors to implement robust cybersecurity controls and practices to secure sensitive data from cyber threats. DFARS 7012 specifically requires defense contractors and subcontractors to do the following:

- Protect unclassified CDI in accordance with NIST SP 800-171. Contractors must implement the 110 security controls and 320 objectives specified in NIST SP 800-171.
- Report cyber incidents to the DoD and provide logs and server access. Contractors must report all cyber incidents to the DoD Cyber Crime Center (DC3), provide malicious software and all cyber incident data, preserve cyber incident data for 90 days, and support DC3 with their cyber investigation.
- Confirm Cloud service providers (CSPs) meet Federal Risk and Authorization Management Program (FedRAMP) moderate or equivalent standards. Contractors must ensure that the CSPs they are currently using have achieved the requirements for a FedRAMP moderate baseline or equivalent standard.
- Flow down to subcontractors. Contractors must flow down

requirements to their subcontractors, meaning their subcontractors are subject to the same requirements.

In addition to DFARS 7012, the following three additional clauses went into effect with DFARS' Interim Final Rule in November 2020:

1. **DFARS 7019:** Improves on DFARS 7012 by making it a requirement for contractors to conduct an NIST SP 800-171 self-assessment aligned with the DoD assessment methodology. It also requires that self-assessment scores be sent to the DoD through its Supplier Performance Risk System (SPRS) [8].
2. **DFARS 7020:** Informs contractors that the DoD possesses the right to conduct a higher-level assessment of a contractor's business operations and cybersecurity compliance. Contractors must provide DoD assessors with full access to their systems, personnel, and facilities. Contractors must also confirm their subcontractors have valid SPRS scores on file [9].
3. **DFARS 7021:** Sets the foundation for the Cybersecurity Maturity Model Certification (CMMC) and requires contractors to have a current (i.e., not older than three years) CMMC certificate at the CMMC level required by the contract and maintain the CMMC certificate at the required level for the duration of the contract [10].

WHAT IS CMMC?

CMMC is the DoD's program to assist industry players in meeting the necessary requirements outlined in DFARS 252.204-7012 and NIST SP 800-171 Rev. 2. The CMMC program intends to provide a consistent assessment methodology prior to contract award that can validate if a potential DoD contractor implements adequate cybersecurity protections for DoD information [11]. The program applies to all contracts where a defense contractor or subcontractor will process, store, or transmit FCI or CUI on their information systems and to new contracts, task orders, delivery orders, solicitations, and as a condition for an option period.

FCI is information not intended for public release that is provided by or generated for the government under a contract to develop or deliver a product or service to the government, defined in FAR 52.204-21 [6]. CUI is information the government creates or possesses or that an entity creates or possesses for or on behalf of the government that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls, defined in 22 Code of Federal Regulations (CFR) Part 2002 [12]. The CUI marking replaces legacy markings such as for official use only (FOUO), sensitive but unclassified (SBU), and law enforcement sensitive (LES) [13].

The CMMC program is designed to align with the existing DoD information security requirements of DIB partners. CMMC's goal is to further enforce the security and protection of sensitive unclassified information and CUI shared by the DoD and its contractors and subcontractors by providing a guarantee that the industry is meeting cybersecurity requirements for future contracts and systems that properly store, process, and transmit CUI [14].

The CMMC program was initially started as CMMC 1.0 in January 2020 but was updated to the next iteration of the cybersecurity model with CMMC 2.0 in November 2021. CMMC 2.0 was designed to reduce the resources required for small- to medium-sized businesses to meet CMMC compliance. One notable way CMMC 2.0 did this was by reducing the number of maturity models in the CMMC program from five in CMMC 1.0 to three for CMMC 2.0.

CMMC's goal is to further enforce the security and protection of sensitive unclassified information and CUI shared by the DoD and its contractors and subcontractors.

The CMMC program is based on DFARS 252.204-7012 and builds upon its concepts, but there are a few major differences that set it apart. The program seeks to add a required verification component that can efficiently verify the cybersecurity of defense contractors consistently relative to FAR 52.204-21, DFARS 252.204-7012, NIST 800-171 Rev. 2, and NIST 800-172. CMMC uses a tiered model (Figure 1) that requires companies that handle sensitive unclassified DoD information to implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the data.

CMMC Level 1 (Foundational)

This level is reserved for all federal contractors and subcontractors that only handle FCI. It protects information and communications related to federal contractors and has 15 cybersecurity requirements from FAR 52.204-21 that must be followed [6]. CMMC Level 1 also requires that a self-assessment be conducted by the organization seeking certification (OSC) and an affirmation that they align with FAR 52.204-21 annually. Results from both the assessment and affirmation must be sent to the SPRS [11].

CMMC Level 2 (Advanced)

This level is designed for DoD contractors and subcontractors that specifically handle CUI. It requires organizations to implement the 110 security controls specified in NIST SP 800-171 Rev. 2, which are the same NIST controls required in DFARS 252.204-7012. CMMC Level 2 also requires OSCs to either conduct self-assessments or have a CMMC Third-Party Assessment Organization (C3PAO) conduct the assessment every three years. The type of assessment organizations choose depends on the type of information processed, transmitted, or stored on the contractor or subcontractor information systems.

The results from contractor self-assessments should be entered into the SPRS, and results from a C3PAO assessment should be entered into the CMMC Enterprise Mission Assurance Support Service (eMASS). All contractors under CMMC Level 2 will have to affirm compliance with the 110 security control requirements featured in NIST SP 800-171 Rev. 2 annually and that affirmation will be entered into the SPRS [11].

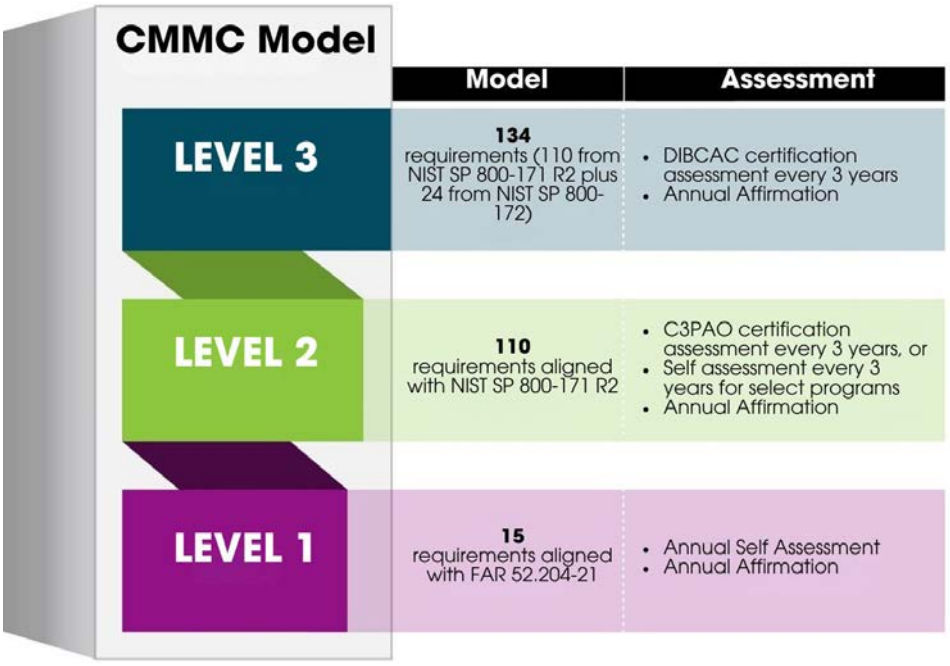


Figure 1. CMMC Certification Levels and Requirements *(Source: U.S. DoD CIO [15]).*

CMMC Level 3 (Expert)

This level is the CMMC final level and meant for DoD contractors and subcontractors that handle the most sensitive CUI for DoD programs with the highest priority. It focuses on reducing a system environment's vulnerabilities to advanced persistent threats (APTs) with more rigorous and advanced cybersecurity measures. CMMC Level 3 requires organizations to properly implement the 110 security controls specified in NIST SP 800-171 Rev. 2 and an additional 24 security controls specified in NIST SP 800-172.

To qualify for this level's certification, an organization must have already demonstrated they are compliant and meet all requirements under CMMC Level 2. At CMMC Level 3, certification must be completed with an assessment by the DoD's own Defense Contract Management Agency Defense Industrial Base Cybersecurity Assessment Center (DCMA DIBCAC) every three years. Assessment results from a C3PAO or DIBCAC should be entered into CMMC eMASS. Affirmations of compliance with NIST 800-171 Rev. 2 and NIST 800-172 are still required annually [11].

SPRS AND CMMC SCORING METHODOLOGY

SPRS is a self-certification scoring method that measures current cybersecurity compliance with the NIST 800-171 framework (Figure 2). The SPRS score is a numerical grade that gets entered into the DoD SPRS application using designated systems. It is a tool that the DoD and contracting officers use to measure the risk associated with a contractor's cybersecurity posture. The DoD now uses the SPRS score as a major component of a contractor's CMMC evaluation. The score must be maintained and cannot be more than three years old [16]. The scoring methodology an organization uses will depend on the CMMC level they operate on. These scores are based on three levels presented in the next paragraphs.

CMMC Level 1

In this level, there is no score, and requirements are "MET" or "NOT MET."

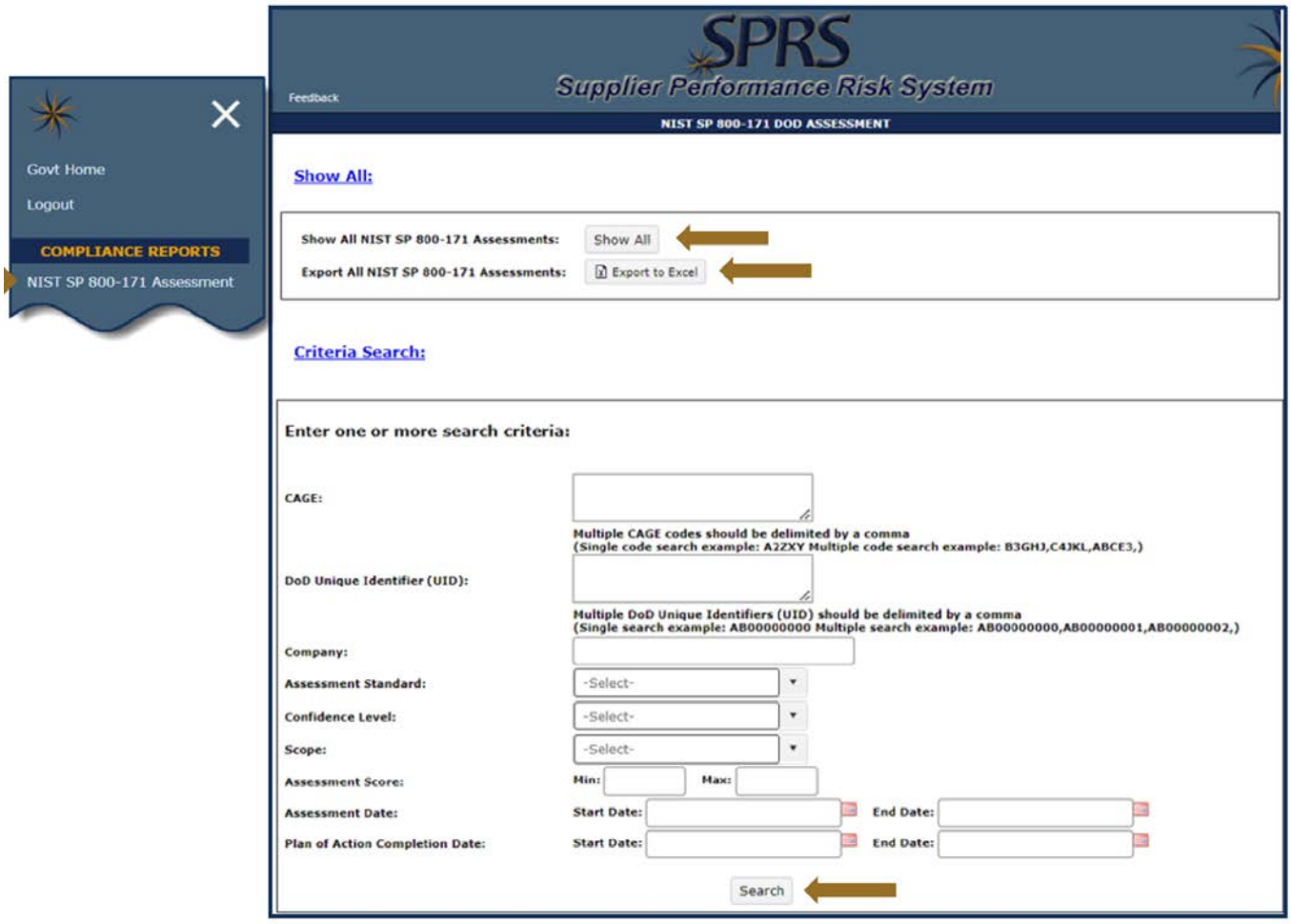


Figure 2. NIST SP 800-171 Assessment Landing Page *(Source: Defense Information Systems Agency [17]).*

CMMC Level 2

The scoring in this level ranges from −203 to 110 points, with a minimum passing score of 88. Security requirements are valued at 1, 3, or 5 points and begins with a perfect score of 110. Points are deducted (1, 3, or 5) for controls not implemented and could go down to −203. Nothing is deducted if the proper security control has been implemented. If all controls are implemented, the perfect score of 110 is maintained.

The following lists the deduction scheme and possible points that can be subtracted:

- If not implemented, this could lead to significant exploitation of the network or exfiltration of CUI (5 points).
- If not completely or properly implemented, this could be partially effective and points adjusted depending on how the security requirement is implemented (3 or 5 points).
  - Partially effective implementation (3 points).
  - Noneffective (not implemented at all) (5 points).
- If not implemented, this has a specific and confined effect on the security of the network and its data (3 points).
- If not implemented, this has a limited or indirect effect on the security of the network and its data (1 point).

CMMC Level 3

The scoring in this level has a maximum score of 24, with each security requirement valued at 1 point. If any single requirement is not met, it will result in a failed CMMC Level 3 assessment [18].

Results at all levels are entered into the SPRS and reviewed by contracting officers and requiring activities.

WHY THE NEED FOR CMMC?

The world has seen constant technological advancements in artificial intelligence, machine learning, automation, Cloud Computing, Edge Computing, the Internet of Things (IoT), and networking capabilities over the past decade. This ever-changing cyber landscape has also allowed for the advancement of cyber threats such as malware, distributed denial-of-service attacks, ransomware, social engineering attacks, phishing, injection attacks, and supply chain attacks. This change has increased the overall threat landscape organizations must handle daily and bolstered the tools cyber adversaries have at their disposal. Attackers are regularly and exponentially outsmarting state-of-the-art cyber defenses of businesses, institutions, and governments, leaving them ahead of cyber professionals [19].

According to Statista, the global cost of cybercrime is projected to rise from $9.22 trillion in 2024 to $13.82 trillion by 2028 [20]. In MoreField's cybersecurity forecast for 2025, ransomware attacks have also been the highlight of emerging threats, with their frequency and complexity on the rise [21]. This forecast states that ransomware has demonstrated an 81% year-over-year increase from 2023 to 2024.

> ***The global cost of cybercrime is projected to rise from $9.22 trillion in 2024 to $13.82 trillion by 2028.***

In 2023, the Cyber National Mission Force carried out 22 operations. In comparison, the Cyber National Mission Force has been deployed more than 85 times to carry out missions spanning across at least 80 networks in 2024, according to Morgan Adamski, executive director of the U.S. Cyber Command [22]. Cyber Command's expanded operations come amid intensifying threats from foreign adversaries like China, which federal agencies warn has been carrying out broad and significant cyber espionage campaigns targeting top government officials in the United States.

Nation-state actors and APTs are active on the world stage and can generate and impact global conflicts, fueling tension between nations. The Federal Bureau of Investigation, Cybersecurity

and Infrastructure Security Agency (CISA), and National Security Agency (NSA) assessed that cyber actors affiliated with the Russian General Staff Main Intelligence Directorate (GRU) 161st Specialist Training Center (Unit 29155) have been responsible for computer network operations against global targets for espionage, sabotage, and reputational harm since at least 2020. GRU Unit 29155 cyber actors began deploying the destructive WhisperGate malware against multiple Ukrainian victim organizations as early as January 13, 2022 [23].

In March 2024, hackers that operated as part of the APT31 hacking group in support of the People's Republic of China's Ministry of State Security were charged with conspiracy to commit computer intrusions and wire fraud [24]. This was the result of their involvement in conducting global campaigns of computer hacking that targeted political dissidents and perceived supporters located inside and outside of China, government and political officials, candidates, and campaign personnel in the United States and elsewhere. APT31 sent over 10,000 malicious emails that included a malicious tracking link to government officials and journalists from prominent news outlets and gained access to the victim's computer networks using sophisticated zero-day exploits.

These cyber events and statistics show that there is a yearly increase in the frequency of cyberattacks, highlighting the increased activity of cyber adversaries and nation-state actors and need for organizations to be prepared in today's cyber landscape.

> ***APT31 sent over 10,000 malicious emails that included a malicious tracking link to government officials and journalists from prominent news outlets and gained access to the victim's computer networks using sophisticated zero-day exploits.***

In the 2019 DoD Office of Inspector General (DODIG) Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems, it was found that DoD contractors did not consistently implement DoD-mandated system security controls for safeguarding defense information [25]. Within the contractors assessed by the DODIG, they identified multiple deficiencies regarding the use of multifactor authentication (MFA), enforcing strong password use, identifying and mitigating network/system vulnerabilities, documenting cyber incidents, implementing physical security controls, overseeing network and boundary protection services provided by a third-party company, protecting CUI on removable media, and more. In this audit, it was noted that there was not a specific established process for verifying a contractor's networks and systems. It was also noted that DoD component contracting offices and requiring activities did not always know which contracts required contractors to maintain CUI because the DoD did not implement processes and procedures to track which contractors maintained CUI.

In December 2024, the U.S. Treasury Department stated that a China-based APT actor broke into their systems and was able to access employee workstations and some unclassified documents [26]. The Treasury Department determined this breach to be a major cyber incident where the APT was able to override security via a key used by a third-party service provider, BeyondTrust, who offered remote technical support to their employees.

The DODIG audit and Treasury Department breach show that DoD and government agencies need to seriously improve their operational practices to be more secure and highlight the importance of properly securing sensitive unclassified information and CUI. These events also emphasize the fact that APTs can intentionally target sensitive unclassified information and CUI in their cyber operations and will leverage third-party service providers to gain access to critical systems.

The CMMC program provides clear cybersecurity requirements that are tried, true, and known as best practices. The program gives DoD contractors a clear set of goals they should strive for in terms of meeting all requirements featured in FAR 52.204-21, DFARS 252.204-7012, NIST 800-171, or NIST 800-172 and implementing the proper security controls into their systems.

The CMMC program also plans to ensure the DoD and its contractors and subcontractors are doing their due diligence in applying proper security controls and reviewing its own cybersecurity. Requiring cybersecurity assessments every three years and annual affirmations to confirm compliance with the respective CMMC level can be seen as a form of ongoing monitoring for the cybersecurity practices of DoD contractors and subcontractors. The program directly addresses many of the security faults and issues mentioned in the DODIG audit, promotes the protection of sensitive unclassified data and CUI, prepares organizations to better respond to cyber threats and APTs, and aims for improving the cybersecurity posture of the DIB. While not every DIB company will necessarily be subject to a CMMC mandate, most eventually will. To be successful, the CMMC initiative relies on an entire community of security and training professionals [27].

THE CMMC ECOSYSTEM

Throughout the CMMC process from start to finish, there are various organizations and entities that an OSC may interact with for CMMC compliance. The CMMC ecosystem refers to the interrelated processes, organizations, and entities that are involved in the initial review, implementation, assessment, and certification of the CMMC framework.

DoD Chief Information Officer (CIO) CMMC Project Management Office

The DoD CIO provides oversight of the CMMC program and establishes CMMC assessment, accreditation, and training requirements; develops and updates CMMC program policies; implements guidance; and establishes DoD requirements for C3PAOs, the Cybersecurity Assessor and Instructor Certification Organization (CAICO), assessors, and instructors [28].

DCMA DIBCAC

This center advises DoD CIO CMMC Project Management Office (PMO), conducts CMMC Level 2 certification assessments on C3PAOs, and conducts CMMC certification assessments on DIB.

CMMC Accreditation Body (Cyber AB)

This is the official accreditation body of the CMMC ecosystem and the sole authorized nongovernmental partner of the DoD in implementing and overseeing the CMMC program [29].

C3PAO

These are organizations authorized by the Cyber AB to perform official CMMC assessments. They employ CMMC assessors and are responsible for conducting the assessments and issuing CMMC certifications to organizations that meet the requirements [30].

Certified CMMC Professional (CCP)

These are qualified individuals or organizations authorized by the Cyber AB to evaluate and assess organizations against the CMMC framework for Level 1.

Certified CMMC Assessor (CCA)

These are qualified individuals or organizations authorized by the Cyber AB to evaluate and assess organizations against the CMMC framework for Level 2.

Both CCP and CCA conduct on-site or remote assessments to determine if an organization meets the required cybersecurity practices and processes for certification.

CAICO

CAICO is the dedicated CMMC entity facilitating the training, examination, and professional certification for individuals within the CMMC ecosystem [30].

Licensed Training Provider (LTP)

LTP is an established training organization that has been reviewed and approved by CAICO. The organizations that fall under this provider deliver CMMC-related training and education programs, equipping individuals and organizations with the necessary skills and knowledge to meet CMMC requirements. They offer specialized courses and certifications to enhance cybersecurity expertise.

Licensed Publishing Provider (LPP)

Vetted by CAICO, this organization is responsible for creating quality CMMC training curriculum that is utilized by LTPs to individuals pursuing official DoD-recognized, CMMC, professional certifications.

Certified CMMC Instructor

This includes individuals that work with LPP and LTP to develop curriculum and deliver courses.

Noncertified Entities

These are organizations or professionals that can assist in preparing OSCs for CMMC assessments but are not certified to conduct official CMMC assessments.

Registered Practitioner Organization (RPO)

RPO is an organization that provides a noncertified advisory service, often before CMMC assessment. RPOs do not conduct certified CMMC assessments.

Registered Practitioners (RPs)

RPs are individuals with implementation experience who provide consultative preparation services to OSCs and work under an RPO [30].

REACHING COMPLIANCE AND PREPARING FOR ASSESSMENT

When beginning to initiate the path to CMMC compliance, OSCs should do the following:

1. *Look to engage with familiar DoD organizations for assistance.*
2. *Establish a procurement account and obtain an active CMMC status in the SPRS.*
3. *Understand the scope of CMMC. OSCs must look inward to see where they stand within the overall CMMC process.*

   First, there must be an understanding of the CMMC levels, what is required, and what they entail. OSCs need to take note of the type of data they handle in their operations and whether it is FCI or CUI. If the organization only handles FCI, follow the requirements featured in CMMC Level 1. If they handle CUI, then the organization should focus on whether they fall under Level 2 or 3.

   Reviewing contract requirements, understanding how critical and high priority an organization's work is, and evaluating the risk of an organization's threat environment for cyberattacks and APTs will help determine whether an organization will follow Level 2 or 3 requirements. Understanding the CMMC scoring methodology will also be key. For example, OSCs at CMMC Level 2 can only afford to lose 22 points through deduction while still being compliant.

4. *Understand the scope of the assessment.*

   OSCs need to identify their assets and exactly where the FCI or CUI resides within the organization. In this case, an asset is anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (installed and physical

instances), virtual computing platform (common in Cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards, etc.) [31]. FCI and CUI data can be located on local storage, Cloud storage, printers, servers, workstations, IoT devices, and mobile devices. Attention should be paid to when and how FCI or CUI is processed, stored, and transmitted in and out of the organization during operations as follows:

- Process – FCI/CUI can be used by an asset (accessed, entered, edited, generated, manipulated, or printed).
- Store – FCI/CUI is inactive or at rest on an asset (located on electronic media, in system component memory, or in physical format like paper documents).
- Transmit – FCI/CUI is being transferred from one asset to another.

With the knowledge and understanding of the location of FCI/CUI data and the nature of operational processes, a network topology diagram should be created of how FCI or CUI moves within the organization to better visualize what is being protected.

Instead of maintaining a fully fleshed-out network environment, an organization may opt to use an on-premise or Cloud enclave for CUI. Enclaves are stand-alone information systems that establish a software-defined perimeter around their included resources to protect sensitive data such as CUI of an organization's information systems [32]. This creates a network partition and allows incorporating NIST 800-171 for FCI/CUI in specific areas of a network and for related operations.

Organization Maintained Enclave

A few advantages and disadvantages related to organization maintained enclaves are as follows:

- Advantages
  - Lowers cost of implementation
  - Allows for quicker implementation
  - Limits use of CUI-related assets (workstations, phones, etc.)
  - Easier to reach security requirements
  - Reduces continuous monitoring workload
- Disadvantages
  - Limited assets could restrict business operations
  - More susceptible to insider threats
  - Air-gapped - physically isolated from other networks and any external connections, including the public internet

An organization may also opt to use a third-party CSP or managed service provider (MSP). DFARS 252.204-7012 requires the use of FedRAMP-approved government Clouds. FedRAMP was created in 2011 to present a cost-effective, risk-based approach for adopting secure Cloud services across the federal government by providing a standardized approach to security and risk assessment for Cloud technologies and federal agencies. According to FedRAMP, compliance is required for all Cloud service providers that offer services to federal agencies and all federal agencies that transmit sensitive data over the Cloud. FedRAMP helps eliminate redundant and inconsistent efforts, supports the adoption of Cloud Computing and innovative technologies, and promotes the use of properly secured systems and applications.

FedRAMP helps eliminate redundant and inconsistent efforts, supports the adoption of Cloud Computing and innovative technologies, and promotes the use of properly secured systems and applications.

Managed Service Provider Cloud

A few advantages and disadvantages related to managed service provider Cloud environments are as follows:

- Advantages
  - Lower cost of system management (pay only for what is needed)
  - Expertise and experience from MSP team
  - High system uptime and availability
  - Ease of scalability
- Disadvantages
  - Lack of on-site support
  - Subject to vulnerabilities of MSP, such as access controls and uncontrollable administrative rights
  - Depends on MSP for technical assistance, patches, and updates

OSCs also want to take note of who has access to stored FCI/CUI and who has authorization to process and transmit FCI/CUI. The following questions should be asked:

- Who are the contract information systems officers?
- Who writes the procedures and policies?
- Who will monitor logs, access, and user permissions?
- Who will implement technical changes, such as patches/updates?
- Who will train employees?
- Who will monitor the organizational alignment with current procedures and policies?
- Are they employees, and are they part time or full time?
- Are individual network environments maintained, or is an MSP utilized for FCI/CUI-related operations?

In continuing to initiate the path to CMMC compliance, OSCs should also do the following:

1. *Conduct a self-assessment.*
   Based on the understanding of the CMMC requirements, current cybersecurity posture, and how FCI/CUI flows in and out of OSCs, a self-assessment can be conducted.
   An RPO can also be utilized to assess the state of OSCs before an official assessment. Are the proper security practices and controls in place relative to the requirements of FAR 52.204-21, DFARS 252.204-7012, NIST 800-171, or NIST 800-172? Using CMMC's scoring methodology, what score did the OSC receive?
2. *Develop a plan to reach full CMMC compliance.*
   Based on the score in the initial self-assessment, where can OSCs improve their security posture? OSCs need to weigh their options, prioritize what security issues need to be addressed, and develop a plan to improve security control. Does MFA or encryption need to be enabled for certain business functions? Do cyber professionals need to be hired? How do security controls affect CMMC scoring?

   For example, OSCs at Level 2 may be deducted 5 points for missing a security control like MFA. OSCs may be limited in their ability to implement a complete fix but could possibly implement a control that will deduct fewer points. These changes can move the needle in improving overall cybersecurity and CMMC score.
3. *Submit the assessment scope to the assessor.*
   Formally document and provide the CMMC assessor with the full scope of assets, facilities, systems, and people involved with FCI/CUI business operations. These are the assets that will be reviewed during the official CMMC assessment.
4. *Display CMMC readiness and remediation.*
   Carry out the plan that was created to reach CMMC compliance and remediate any high-priority shortcomings in previous organizational security controls and processes.
5. *Obtain a C3PAO assessment or conduct an official self-assessment.*
   Once remediations have occurred, OSCs are ready for the official CMMC assessment. This can be conducted by a C3PAO, CCP, or CCA, depending on CMMC requirements. In-house personnel can conduct the official self-assessment, but they must be qualified by the Cyber AB.
6. *Pass or fail certification.*

The CMMC process can take organizations anywhere from 16 to 24 months to fully complete. The timeframe will depend on the current

state and complexity of the assessed environment, and the process can take longer if issues arise along the way. Many organizations that currently process, store, or transfer FCI or CUI are already preparing themselves to align with CMMC requirements. If they are not, it is up to the organization if they would like to continue working with the DoD on future contracts.

> ***Many organizations that currently process, store, or transfer FCI or CUI are already preparing themselves to align with CMMC requirements.***

On October 15, 2024, the final rulings for the Cybersecurity Maturity Model Certification (CMMC), officially known as Title 48 CFR and Title 32 CFR Part 170, were published [11]. These rulings became effective on December 16, 2024, 60 days after the publication of the final rule. CMMC assessment requirements will be implemented using a four-phase plan over three years (see Figure 3). The phases add CMMC level requirements incrementally, starting with self-assessments in Phase 1 and ending with full implementation of program requirements in Phase 4 [33].

- **Phase 1** was extended by six months and started with the implementation of the October 15, 2024, ruling and amendments to the DFARS clause, which occurred on December 16, 2024.
- **Phase 2** will require contractors handling CUI in most circumstances to undergo a third-party assessment by a C3PAO as a condition of award. Phase 2 is estimated to go into effect December 16, 2025.
- **Phase 3** will require DoD's DCMA DIBCAC to conduct Level 3 CMMC assessments for contracts related to the most sensitive CUI. Phase 3 is estimated to go into effect December 16, 2026.
- **Phase 4** is the "full implementation" of the CMMC requirements. Phase 4 is estimated to go into effect December 16, 2027.
- **Phases 2–4** will each start consecutively one calendar year after the preceding phase. However, the DoD's objective timeline to begin implementing the CMMC requirements is fiscal year 2025.

Figure 3. The Planned Implementation Phases of the CMMC Program *(Source: U.S. DoD CIO [34]).*

- Full implementation of CMMC by all defense contractors is estimated to occur over seven years.

RESOURCES TO HELP IN REACHING CMMC COMPLIANCE

Cyber AB Marketplace

Provides a trusted location to look up potential RPO, CCA, CCP, C3PAO, LTP, and LPP [35].

FedRAMP Marketplace

A searchable and sortable list of Cloud providers, products, and services that are FedRAMP and Defense Information Systems Agency (DISA) approved [36].

NSA DIB Cybersecurity Services

NSA offers no-cost cybersecurity services to any company that contracts with the DoD (sub or prime) or has access to nonpublic DoD information. These services include protective Domain Name System (DNS) (a DNS filter), vulnerability scanning, attack surface management, and access to nonpublic, DIB-specific NSA threat intelligence [37].

DC3 DIB Collaborative Information Sharing Environment (DCISE)

An operational hub of the DoD's DIB Cybersecurity Program that is the designated recipient for reporting DIB cyber incident reports as required by 10 U.S. Code Sections 391 and 393 and DFARS 252.204-7012.

DC3 DCISE offers no-cost forensics, malware analysis, and cybersecurity services for DIB partners. It also shares a significant number of cyber threat reports (hundreds annually) for DIB and U.S. government consumption [38].

NIST Manufacturing Extension Partnership (MEP)

The NIST MEP is a national network with hundreds of specialists across MEP centers located in all 50 states and Puerto Rico, as shown in Figure 4. MEP provides companies with services and access to public and private resources to enhance growth, improve productivity, reduce costs, and expand capacity. The NIST MEP can help DIB organizations assess their business's current risk posture, identify any gaps, and implement solutions to cost effectively protect digital and

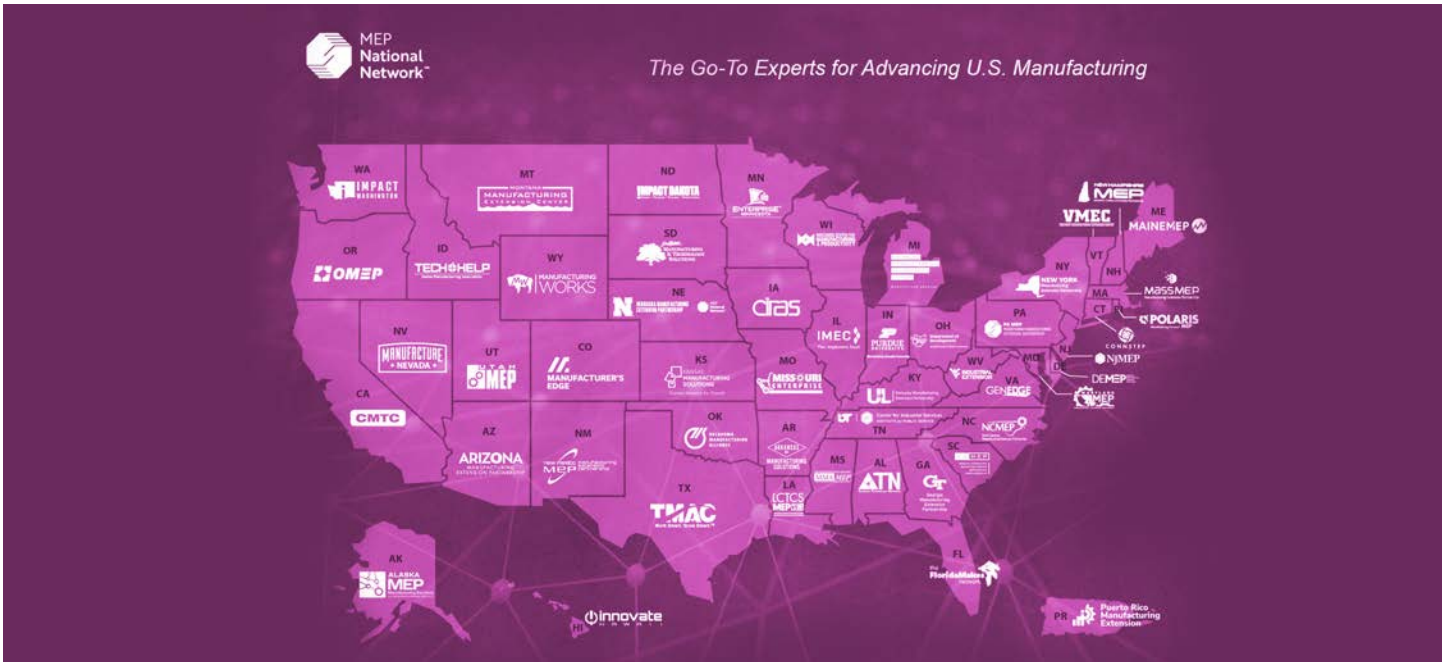


Figure 4. MEP National Network Map *(Source: NIST [40])*.

information assets and meet legal and contractual cybersecurity and privacy requirements [39].

Next Gen Commercial Operations in Defended Enclaves for Small Businesses (N-CODE)

The N-CODE program was created to improve cybersecurity while lowering the barrier for small businesses to engage with DoD programs. Small businesses may find that individually implementing security controls and then demonstrating CMMC compliance are cost prohibitive. As such, small businesses that opt into the N-CODE pilot can leverage an initial set of productivity tools within a secure environment that will meet a majority of the CMMC controls. This will provide an affordable path to secure data while maximizing participation in the defense industrial base [41].

CONCLUSIONS

The CMMC program represents a significant shift in how the DoD and DIB approach cybersecurity within its supply chains. Driven by the escalating cyber threat landscape and vulnerabilities exposed by past incidents, APT activity is becoming increasingly more prominent. CMMC aims to establish an agreeable and verifiable baseline level of security for handling sensitive unclassified government information and CUI. CMMC also provides an official process of confirming a baseline of cybersecurity at the contract level. The program's tiered structure, ranging from basic cyber hygiene at Level 1 to advanced threat protection at Level 3, allows the DoD to tailor requirements based on the sensitivity of the data handled by each contractor.

While achieving CMMC compliance requires a significant investment of time and resources, the framework provides a clear roadmap for organizations to enhance their cybersecurity posture. By understanding the requirements, conducting thorough self-assessments, leveraging helpful organizations, and developing comprehensive remediation plans, contractors can meet compliance obligations and strengthen their overall defenses against increasingly sophisticated cyber threats. Ultimately, CMMC aims to create a more secure and resilient DIB that is better equipped to protect critical information and maintain national security. ■

REFERENCES

[1] The White House. "Executive Order 13556 – Controlled Unclassified Information." https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information, accessed on 7 February 2025.

[2] NIST. "NIST Released Special Publication 800-171, Revision 1, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." https://csrc.nist.gov/news/2016/nist-released-special-publication-800-171,-revisio, accessed on 7 February 2025.

[3] Carnegie Mellon University. "NIST 800-171 Compliance information." https://www.cmu.edu/iso/compliance/800-171/index.html, accessed on 7 February 2025.

[4] NIST. "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." https://csrc.nist.gov/pubs/sp/800/171/r3/final, accessed on 7 February 2025.

[5] NIST. "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171." https://csrc.nist.gov/pubs/sp/800/172/final, accessed on 7 February 2025.

[6] U.S. General Services Administration (GSA). "Basic Safeguarding of Covered Contractor Information Systems." https://www.acquisition.gov/far/52.204-21, accessed on 7 February 2025.

[7] U.S. GSA. "Safeguarding Covered Defense Information and Cyber Incident Reporting." https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting, accessed on 7 February 2025.

[8] U.S. GSA. "Notice of NISTSP 800-171 DoD Assessment Requirements." https://www.acquisition.gov/dfars/252.204-7019-notice-nistsp-800-171-dod-assessment-requirements, accessed on 7 February 2025.

[9] U.S. GSA. "NIST SP 800-171DoD Assessment Requirements." https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements, accessed on 7 February 2025.

[10] U.S. GSA. "Cybersecurity Maturity Model Certification Requirements." https://www.acquisition.gov/dfars/252.204-7021-cybersecurity-maturity-model-certification-requirements, accessed on 7 February 2025.

[11] U.S. DoD CIO. "About CMMC." https://dodcio.defense.gov/cmmc/About/, accessed on 7 February 2025.

[12] Code of Federal Regulations. "Title 32 Subtitle B Chapter XX Part 2002 Subpart A Section 2002.4." https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2002/subpart-A/section-2002.4, accessed on 7 February 2025.

[13] U.S. Department of Commerce Office of the Chief Information Officer. "Controlled Unclassified Information (CUI)." https://www.commerce.gov/ocio/programs/controlled-unclassified-information-cui, accessed on 25 February 2025.

[14] Defense Counterintelligence and Security Agency. "Cybersecurity-Maturity-Model-Certification-CMMC." https://www.dcsa.mil/Industrial-Security/Controlled-Unclassified-Information-CUI/Cybersecurity-Maturity-Model-Certification-CMMC/, accessed on 7 February 2025.

[15] U.S. DoD CIO. "CMMC Certification Levels and Requirements." https://dodcio.defense.gov/cmmc/About/, accessed on 7 February 2025.

[16] DISA. "Supplier Performance Risk System." https://www.sprs.csd.disa.mil/, accessed on 7 February 2025.

[17] DISA. "NIST SP 800-171 Assessment Landing Page." https://www.sprs.csd.disa.mil/pdf/SPRS_Government.pdf, accessed on 25 February 2025.

[18] Code of Federal Regulations. "CMMC Scoring Methodology." https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-D/section-170.24, accessed on 7 February 2025.

[19] de Nobrega, K. M., A. F. Rutkowski, and C. Saunders. "The Whole of Cyber Defense: Syncing Practice and Theory." *The Journal of Strategic Information Systems*, vol. 33, no. 4, https://www.sciencedirect.com/science/article/pii/S096386872400043X, accessed on 7 February 2025.

[20] Fleck, A. "Cybercrime Expected to Skyrocket in Coming Years." Statista, https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/, accessed on 7 February 2025.

[21] Morefield. "5 Cybersecurity Predictions for 2025." https://morefield.com/blog/5-cybersecurity-predictions-for-2025/, accessed on 7 February 2025.

[22] Riotta, C. "U.S. Cyber Force Surges Global Operations Amid Rising Threats." Bank Info Security, https://www.bankinfosecurity.com/us-cyber-force-surges-global-operations-amid-rising-threats-a-26889, accessed on 7 February 2025.

[23] CISA. "Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure." https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a, accessed on 7 February 2025.

[24] U.S. Department of Justice. "Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians." https://www.justice.gov/archives/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived, accessed on 7 February 2025.

[25] U.S. DoDIG. "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems DODIG-2019-105." https://www.dodig.mil/reports.html/Article/1916036/audit-of-protection-of-dod-controlled-unclassified-information-on-contractor-ow/, accessed on 7 February 2025.

[26] Tidy, J., and N. Yousif. "U.S. Treasury Says it was Hacked by China in 'Major Incident'." *BBC*, https://www.bbc.com/news/articles/c3weye2j0e7o, accessed on 7 February 2025.

[27] Cyber AB. "An Ecosystem of Cybersecurity Professionals." https://cyberab.org/CMMC-Ecosystem/The-Cybersecurity-Ecosystem, accessed on 7 February 2025.

[28] Code of Federal Regulations. "Title 32 Subtitle A Chapter I Subchapter Part 170 Subpart B Section 170.6 CMMC PMO." https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-B/section-170.6, accessed on 7 February 2025.

[29] Cyber AB. "About Us." https://cyberab.org/About-Us/Overview, accessed on 7 February 2025.

[30] Cyber AB. "Professions of the Ecosystem." https://cyberab.org/CMMC-Ecosystem/Ecosystem-Roles, accessed on 7 February 2025.

[31] NIST. "Specification for Assets Identification 1.1." https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7693.pdf, accessed on 25 February 2025.

[32] Stiles, S. "What Is a CUI Enclave and When Should You Have One?" https://www.summit7.us/blog/what-is-a-cui-enclave-and-when-should-you-have-one, accessed on 7 February 2025.

[33] Chamberlain, A. "Final CMMC Rule: Key Details and Phased Implementation Timeline." CohnReznick, https://www.cohnreznick.com/insights/final-cmmc-rule-key-details-and-implementation-timeline, accessed on 7 February 2025.

[34] U.S. DoD CIO. "The Planned Implementation Phases of the CMMC Program." https://dodcio.defense.gov/cmmc/About/, accessed on 25 February 2025.

[35] Cyber AB. "Cyber AB Marketplace." https://cyberab.org/Catalog#!/c/s/Results/Format/list/Page/1/Size/9/Sort/NameAscending, accessed on 7 February 2025.

[36] Federal Risk and Authorization Management Program. "FedRAMP Marketplace." https://marketplace.fedramp.gov/products, accessed on 7 February 2025.

[37] NSA. "DIB Cybersecurity Services." https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/DIB-Cybersecurity-Services/, accessed on 7 February 2025.

[38] DoD Cyber Crime Center. "Defense Industrial Base Collaborative Information Sharing Environment Overview." https://www.dc3.mil/Missions/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/, accessed on 7 February 2025.

[39] NIST. "Cybersecurity Resources for Manufacturers." https://www.nist.gov/mep/cybersecurity-resources-manufacturers, accessed on 7 February 2025.

[40] NIST. "MEP National Network Map." https://www.nist.gov/image/mep-national-network-map, accessed on 7 February 2025.

[41] U.S. Army Public Affairs. "Army to Pilot Secure, Cloud Environment for Small Businesses in the Defense Industrial Base." https://www.army.mil/article/280537/army_to_pilot_secure_cloud_environment_for_small_businesses_in_the_defense_industrial_base, accessed on 7 February 2025.

BIOGRAPHY

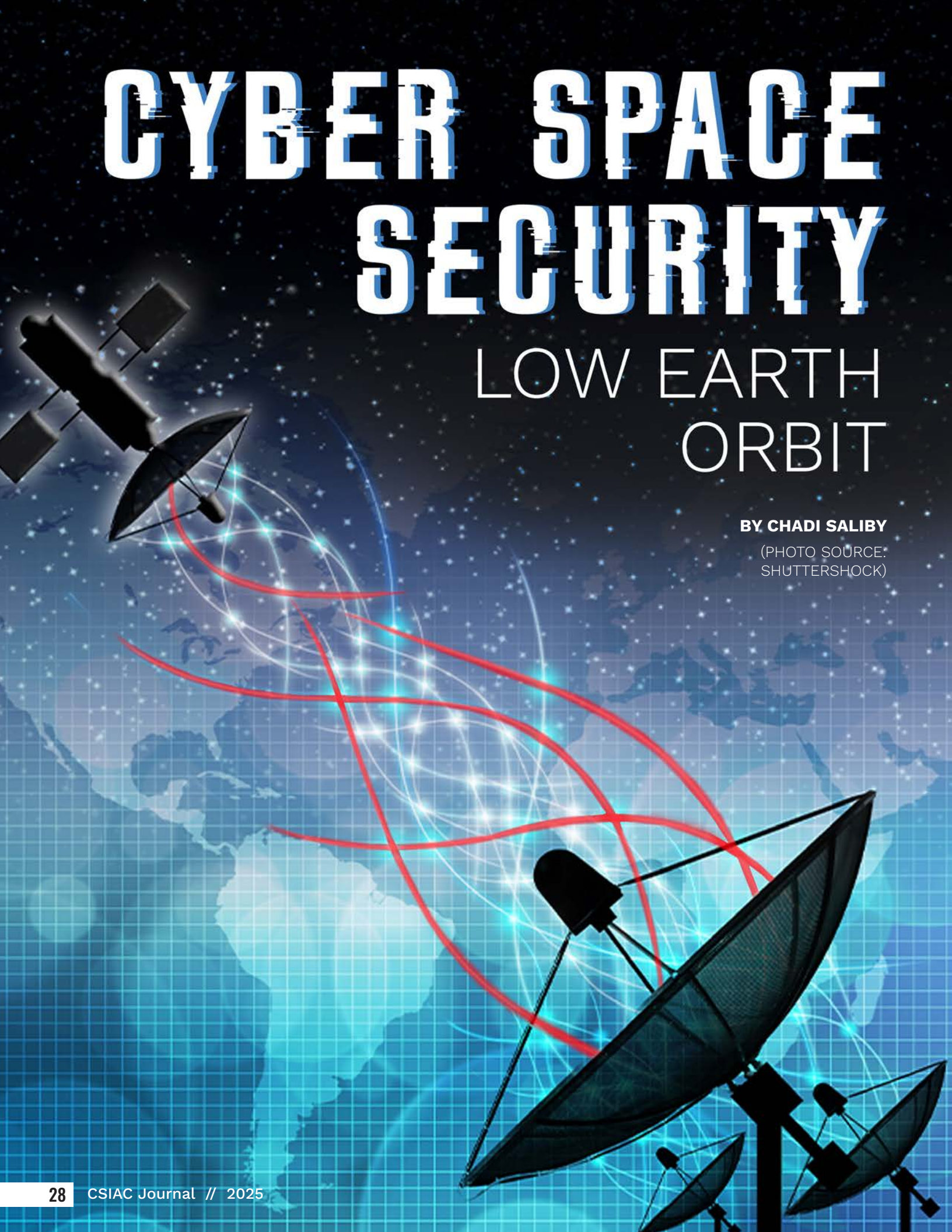
OLUTOYE SEKITERI is a research analyst for the Cybersecurity and Information Systems Information Analysis Center (CSIAC), where he provides research efforts related to CSIAC's four technical focus areas, conducts data analysis to support DoD science and technology communities, and connects government clients with subject matter experts to aid in answering technical inquiries. He previously worked at the University of Maryland, Baltimore County (UMBC) as a research assistant for its Department of Information Systems, supporting a research project recording emergency medical technician stress levels during interactive simulations. Mr. Sekiteri holds a B.S. in information systems from the UMBC, where he is currently pursuing a master's degree in cybersecurity.

CYBER SPACE SECURITY

LOW EARTH ORBIT

BY CHADI SALIBY

(PHOTO SOURCE: SHUTTERSHOCK)



INTRODUCTION

As satellites become increasingly integral to global communication, navigation, and surveillance, targeting their vulnerabilities by malicious actors to disrupt services or gain sensitive information will be imminent to maintain cyberspace security.

Cybersecurity in cyberspace is a versatile field dedicated to safeguarding digital information and infrastructure from a spectrum of cyberthreats and attacks. Cyberspace focuses on protecting the integrity, confidentiality, and availability of satellite systems and their associated data from cyberthreats and attacks.

The importance of cybersecurity controls regarding cyberspace includes robust encryption protocols, secure communication channels, regular system updates, and comprehensive threat monitoring to mitigate risks.

This article will focus on low Earth orbit (LEO), acknowledge medium Earth orbit (MEO) and geostationary Earth orbit (GEO), and discuss the main differences between them (Figure 1).

EXPLORING VARIOUS TYPES OF ORBITS

An orbit is the curved path that an object like a satellite in space takes around another object due to gravity. In space, there is no air and, therefore, no air friction. Because of this, gravity lets the satellite orbit around Earth with almost no further assistance [2].

For cybersecurity specialists, there will be some requirements to understand the basic terminologies regarding satellites' cyber safety and exploring their orbits, as the future of this country and its security depend on it.

As of July 2024, there were 6,281 Starlink satellites in orbit, with a potential to reach 42,000 satellites forming a mega constellation [3] (Figure 2).

LEO

LEOs will be the most accessible part of space for a broad range of operators. Even Amazon Web Services and Microsoft's Azure now provide Ground Station as a Service to enable communication with LEO satellites. LEO will initially host most space-based computing devices, which will require robust cybersecurity measures

> ***For cybersecurity specialists, there will be some requirements to understand the basic terminologies regarding satellites' cyber safety and exploring their orbits, as the future of this country and its security depend on it.***

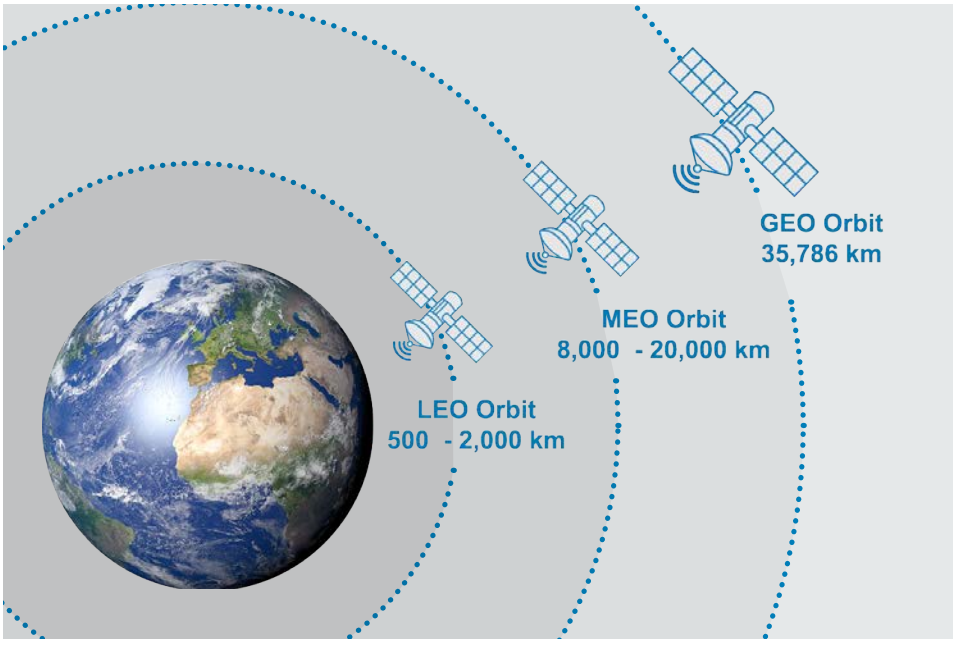


Figure 1. Classification of Satellite Orbits *(Source: Saliby [1])*.

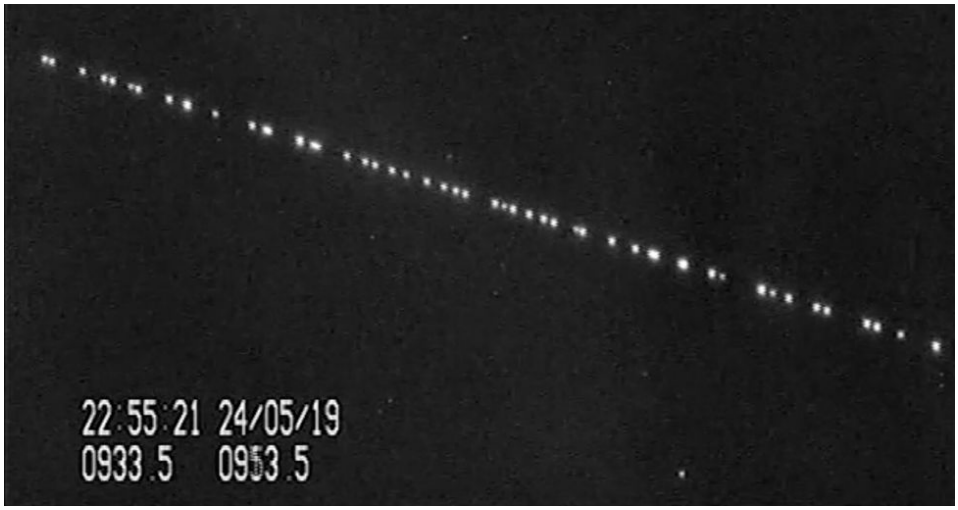


Figure 2. Starlink V2 Satellites Launched From Space Launch Complex 40 (SLC-40) at Cape Canaveral Space Force Station in Florida *(Source: Langbroek [4])*.

and controls, making them a primary target for adversaries.

Any space object that exists in an orbit below an altitude of 2,000 km above Earth is considered a LEO (Figure 1). A popular type of LEO satellites is known as "SmallSats," meaning small satellites [5]. Due to their proximity to Earth, these satellites are extensively utilized for a variety of applications, including telecommunications, Earth observation, and scientific research, leveraging their advantageous low-latency characteristics and enhanced resolution capabilities.

LEOs come in the following wide range of sizes and masses:

- Minisatellite: 100–180 kg
- Microsatellite: 10–100 kg
- Nanosatellite: 1–10 kg
- Picosatellite: 0.01–1 kg
- Femtosatellite: 0.001–0.01 kg

LEO SmallSats' cybersecurity controls are characterized as CubeSats. They are measured by units of U's, where 1U is the equivalent of 10 × 10 × 10 cm [6].

MEO

MEO satellites are higher than the 2,000-km altitude and lower than the GEO satellites. They are primarily recognized for supporting regional coverage in global navigation satellite systems. A historical analysis of the progression of these satellites will provide a more nuanced and thorough understanding of their developing and current capabilities.

The United States initiated the deployment of its Global Positioning System (GPS) in early 1978, with the individual satellites designated as Navstar. It was not until 1982 that the Soviet Union launched its own counterpart, the Global Navigation Satellite System (GLONASS). The Chinese system, known as Beidou (meaning "compass") was introduced later, with its first satellite launched in 2007 [7].

While MEO satellites compare in size to a standard refrigerator or a small car, the size of GEO satellites has significantly evolved since their inception, expanding from a mere few hundred kilograms to over six metric tons today.

GEO

GEO satellites typically range in size from about 1,000 kg (2,200 lb) to over 6,000 kg (13,200 lb) [8]. Their dimensions can vary widely, with some being as large as a car and others as large as a bus. Generally, they have large solar arrays and antennas, which can extend their overall size drastically.

WHY ALTITUDE MATTERS

Satellites traverse earth's orbit due to the intricate equilibrium between gravitational forces and their orbital velocity. Upon launch, a satellite reaches a precise velocity that permits it to perpetually descend toward Earth while advancing forward, thereby achieving a stable orbit.

Since SmallSats are within a certain altitude, they orbit Earth every 60 to 90 min. While MEOs orbit Earth between 8 to 15 hr, GEOs take 24 hr to orbit.

The higher a satellite orbit, the slower it moves. Since GEOs are equatorial orbits, they will be above the same spot over Earth at all times. This is extremely important, as it impacts the windows of communication with ground stations.

SmallSats orbit earth every 90 min, and the window in which they will be visible to their ground stations is only a few minutes. Because they are so close to Earth, they do not consume much energy to get their communication signals to the ground stations or receive instruction commands or a payload patching a vulnerability in their software [9].

THE CYBERSPACE CHALLENGE

When it comes to cyberattacks within cyberspace, there is always a motive and an intention.

Intention denotes the specific plan or goal an individual or a group aims to achieve with their actions, whereas motive encompasses the underlying reasons or drives that inspire those actions. Intentions are typically conscious, while motives can operate at both conscious and subconscious levels.

The cyber risk analysis regarding satellite systems is based on intention and motivation of threat actors and determination of the impact and probability of success undermining the satellite integrity and/or availability. The type of missions conducted by the targeted satellite will dictate the most effective vectors for cyber activity and the subsystems most susceptible to exploitation. These incorporated satellite mission types could be remote sensing or emitting types [10].

Regularly referred to as Earth observation satellites, sensing satellites are specialized satellites designed to collect data regarding the Earth's surface and atmosphere. Sensing is through electromagnetic spectrum sensors, radio waves, infrared radiation, and visible light, which are the same types of data commonly used in internet-based mapping applications or for weather forecasting and meteorological analysis and oceanography.

Emitting satellites are crucial for global communication systems and designed to transmit signals, data, or broadcasts back to Earth or to other satellites. These satellites facilitate the transmission of signals for satellite television services and help provide broadband connectivity to remote areas.

Emitting could also be used in overt or covert operations. Jamming or blocking signals is a classic example of an overt operation targeting other satellites' sensors and performing a communication takeover. Covert operations like spoofing signals are similar to what is seen in electronic warfare.

DEFENDING THE KÁRMÁN LINE

In cybersecurity, one of the most popular and effective cyber defense architectures is defence-in-depth (Figure 3), where there is perimeter

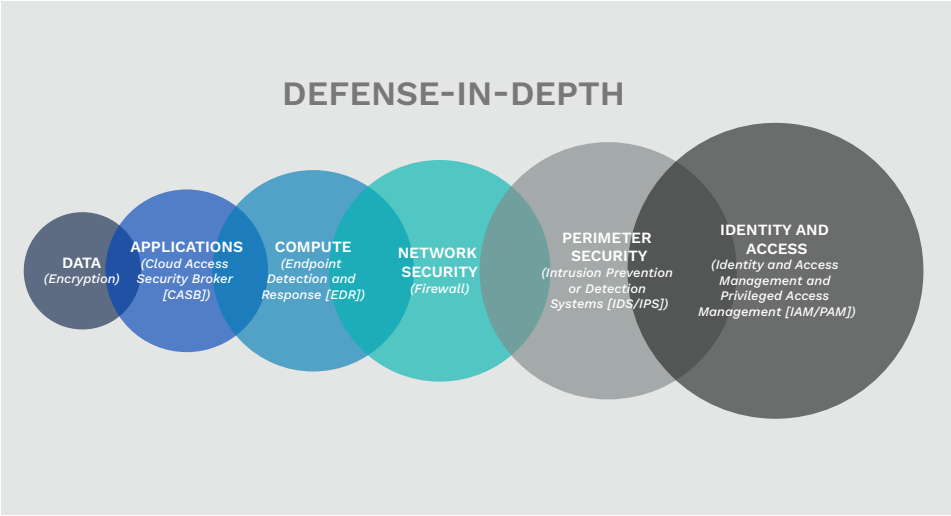


Figure 3. Defence-in-Depth Cybersecurity *(Source: Saliby [1])*.

security. Imagine this perimeter security is the Kármán line, which is the line used for regulatory purposes to differentiate between aircraft and spacecraft spreading a boundary 62 miles or 100 km above mean sea level that borders Earth's atmosphere and the beginning of space [11].

The simplest example of a space system involves a ground-based station device communicating with a space-based device "satellite" where both devices transmit and receive signals (Figure 4).

On the ground-base station, a software-defined radio (SDR) is responsible for receiving various signals like modulation, demodulation, filtering, and encoding and turning them into communications. Providing decryption of the communications stream passes it to a flight control computer running the software that communicates and controls the satellite used for keeping track of its flight operation and trajectory. This provides greater versatility and efficiency in modern communication systems and electronic warfare [6].

An attacker with access to one or more satellites could potentially redirect these satellites to receive commands not only from the legitimate ground station but also from attacker-controlled ones. By configuring a compromised satellite to listen for and accept instructions from a rogue ground station, the threat actor would undermine the integrity of the communication system.

By configuring a compromised satellite to listen for and accept instructions from a rogue ground station, the threat actor would undermine the integrity of the communication system.

SDRs enable cyberattacks to compromise communications either from the ground or the satellite. Both ground stations and space vehicles commonly use SDRs to configure, transmit, and receive signals through their antennas. An attacker could exploit vulnerabilities in these SDRs to disrupt communication streams, either by altering configurations

Figure 4. Satellite Communications Relay *(Source: Canva)*.

or introducing gradual subtle degradation. This kind of attack might not result in an immediate communication shutdown that triggers a rapid response from operators. Instead, it could cause intermittent and unreliable communication between ground and space systems. Consequently, operators might redirect communications to alternative ground stations, affecting the coverage and effectiveness of the space vehicle or its network.

Inadequately implemented encryption jeopardizes confidentiality and creates a misleading sense of privacy and security for the communicating parties. This illusion of protection persists until the parties discover that the secure encryption has been compromised.

Ground-to-space communications encounter augmented risks pertaining to the resilience of encryption. Unlike wired or other mediums, these communications are continuously transmitted through air, making them susceptible to interception. Even though the data is encrypted, the constant and extensive transmission exposes the encryption to potential analysis. An attacker might exploit these frequent and large communication sessions to detect patterns and potentially break the encryption.

CYBERSPACE MITIGATIONS AND CONTROLS

There are many safeguards and controls already incorporated in most satellites. These controls focus on redundancy, with some resilience embedded into their architecture.

A recent analysis conducted by a team of German researchers offers an insightful examination of the security vulnerabilities present in satellites currently orbiting Earth [12]. The researchers, affiliated with Ruhr University Bochum and the Cispa Helmholtz Center for Information Security, scrutinized the software utilized by three small satellites and discovered significant deficiencies in basic protective measures. According to their findings, the satellites assessed exhibited vulnerabilities within their firmware, revealing that minimal security advancements from the past decade have permeated the space domain.

Notably, these satellites lack adequate safeguards concerning who can communicate with their systems and do not incorporate encryption protocols. The researchers suggested that such shortcomings could allow an adversary to seize control of a satellite, posing risks of collision with other objects.

The analysis identified six distinct types of security vulnerabilities across the three satellites, totaling 13 vulnerabilities. Among these are "unprotected telecommand interfaces," which are critical for satellite operators on the ground to communicate with the spacecraft in orbit.

SmallSats and CubeSats

These nanosatellites exhibit heightened vulnerabilities to cyberattacks due to their low construction costs for commercial entities. The proliferation of thousands of satellites in constellations congests LEO, creating fertile ground for malicious actors, especially in conjunction with military satellite deployments. Compromising these satellites could lead to significant economic ramifications and even potential loss of lives.

For instance, by compromising the satellite's navigation system, an

The proliferation of thousands of satellites in constellations congests LEO, creating fertile ground for malicious actors, especially in conjunction with military satellite deployments.

attacker could cause failure in its docking maneuvers or alter its orbital trajectory, potentially redirecting it to face Earth rather than the Sun. This will be explored in the "RoSat Attack" section of this article.

Private Sector and Field-Programmable Gate Arrays (FPGAs)

The private sector has largely neglected cybersecurity, possibly due to a lack of awareness and compounded by the financial burden of adequately securing satellites against cyberthreats and the absence of regulatory frameworks.

Implementing advanced encryption methods like quantum encryption could substantially fortify the cybersecurity of satellites against these threats, coupled with deploying secure gateways reinforced by intrusion prevention systems.

While FPGAs are useful for monitoring systems and overseeing the logic necessary to keep them running with minimal interruption when individual components fail, a complete microcontroller watchdog with logic for failure handling can be implemented in a hardware description language [13]. Invoking or triggering the watchdog scripts or watchdog timer (WDT) by various situations will correct an error in navigation after a certain threshold.

WDT

A WDT is a system monitoring mechanism designed to detect and respond to failures or malfunctions in satellite software or hardware; it could be a lifesaver for SmallSats. The WDT operates by resetting at regular intervals, requiring the system to reset within a specified timeframe to prevent errors or crashes. If threat actors were to disrupt the GPS system from a ground station, a WDT might eventually take over the navigation system, allowing the space system operators to regain control of the space vehicle.

Gold Image

Use of a gold image is another control used in a LEO satellite's cyber arsenal. This image is a preconfigured, standardized snapshot of an operating system with all necessary software and configuration stored onboard the satellite and used in case of a devastating error or failure [14].

Resource Limits

Resource limits are predefined, hard-coded values embedded in the satellite operating system that help to ensure the system's ongoing functionality and extend its operational lifespan. They are predefined thresholds placed on various system resources, such as central processing unit usage, or memory allocation to prevent any single process from consuming excessive resources.

All these cyber controls help protect SmallSats from one of the most dangerous attack types—deorbit [15]. By design, all LEOs are equipped to deorbit and burn up in the atmosphere after a certain number of years. This keeps the amount of space junk floating down. For example, the Starlink satellite's lifespan is approximately five years, in which after that it is programmed to deorbit and burn [2].

> ***By design, all LEOs are equipped to deorbit and burn up in the atmosphere after a certain number of years.***

A threat actor would alter LEOs configuration to manipulate the system to either falsely indicate that the requirements for deorbiting have already been met or modifying the requirements so that deorbit is triggered prematurely based on the new configuration.

SPACE ATTACK RESEARCH AND TACTIC ANALYSIS (SPARTA)

SPARTA is one threat mitigation framework for space attacks. While the SPARTA matrix framework is used to illustrate some examples,

there are also several other key initiatives and agencies focused on cyberspace security, including the Space Information Sharing and Analysis Center, the Defense Advanced Research Projects Agency, and the European Space Agency (ESA).

Addressing the information and communication barriers that hinder the identification and sharing of space-system tactic, techniques, and procedures, SPARTA provides unclassified information to space professionals about how spacecraft may be compromised via cyber and traditional counterspace means (Figure 5). The matrix defines and categorizes commonly identified activities that contribute to spacecraft compromises [16].

For example, the "Initial Access" for the "Compromise Ground System" technique is comprised of two subtechniques: "Compromising On-Orbit Update" and "Malicious Commanding via Valid GS" (Figure 6).

SELECTING COMPROMISING ON-ORBIT UPDATE

The mapping to NIST SP 800-53 Rev5, D3FEND, and ISO27001 makes it very accessible for cybersecurity teams to embed into their cyber programs and understand exactly which countermeasures they need to apply.

If these techniques (Figure 7) were applied properly, RoSat, the first cyberspace incident mentioned next, would have been easily avoided.

CYBERSPACE INCIDENTS

The ability to disable or destroy satellites through cyber exploitation is no longer theoretical—it is a present and growing threat. As space-based infrastructure becomes increasingly vital for communication, navigation, surveillance, and national security, cyberattacks targeting these assets represent one of the most disruptive and potentially devastating threats of the 21st century. Such attacks can compromise sensitive data, disable critical systems, or even render entire satellite constellations inoperable, with far-reaching consequences for both civilian and military operations.

> ***The ability to disable or destroy satellites through cyber exploitation is no longer theoretical—it is a present and growing threat.***

RoSat Attack

In late 1998, a joint German and U.S. X-ray sensor satellite known as Röntgensatellit (RoSat) was compromised [17]. The compromise

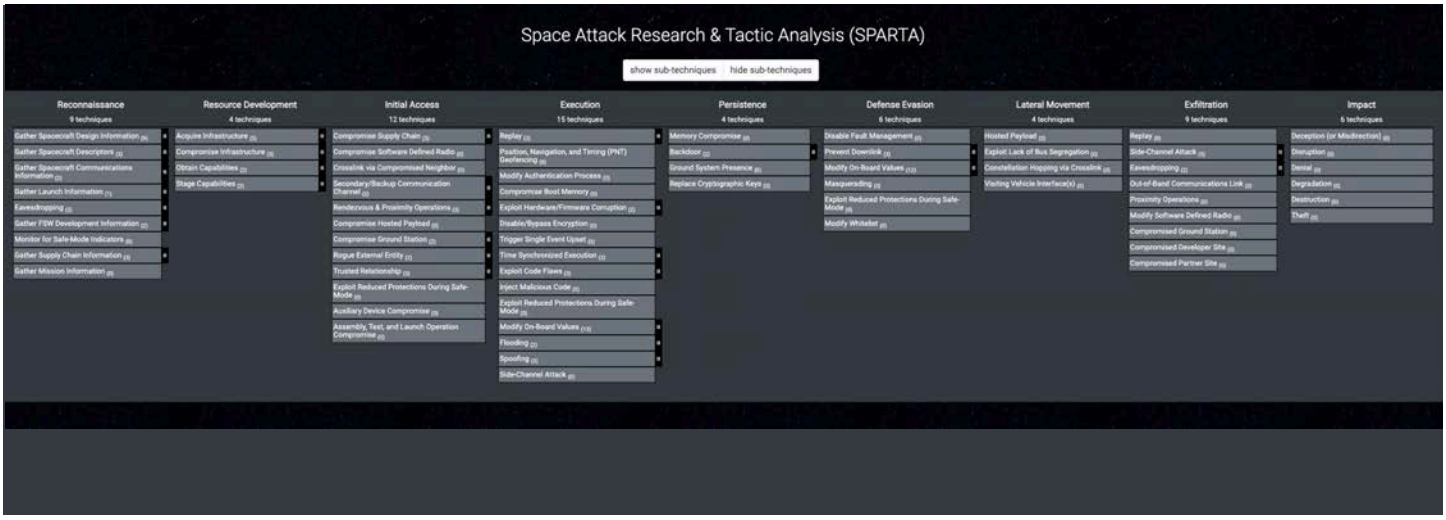


Figure 5. SPARTA Tactics and Techniques Matrix *(Source: Saliby [1]).*

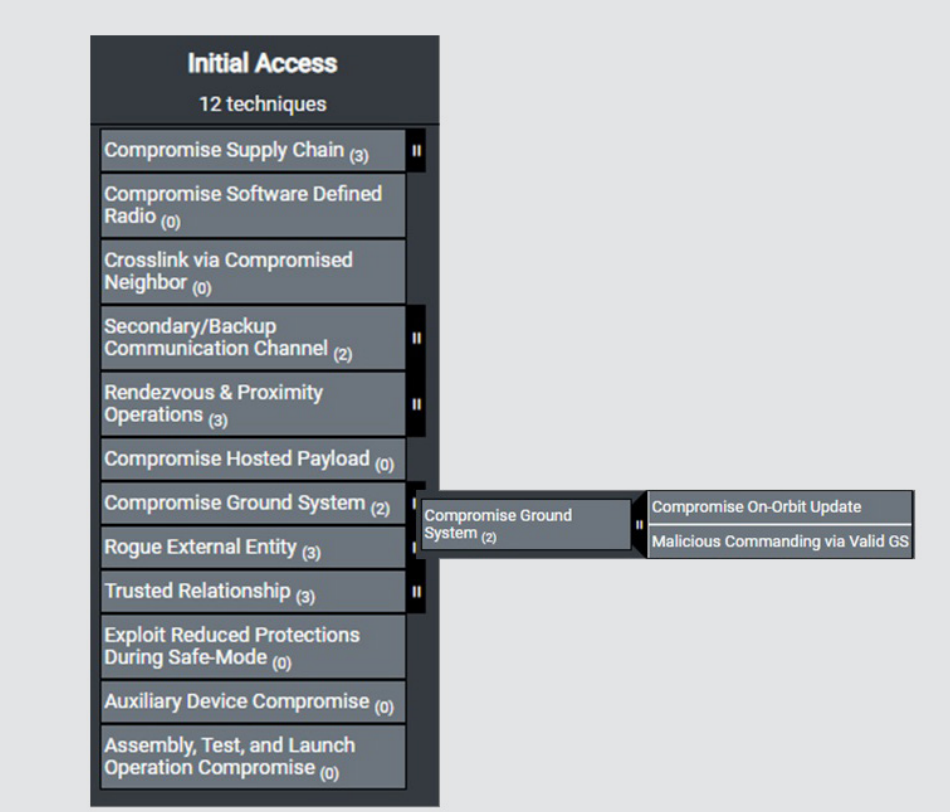


Figure 6. Initial Access Tactic - Compromised Ground System Technique *(Source: Saliby [1])*.

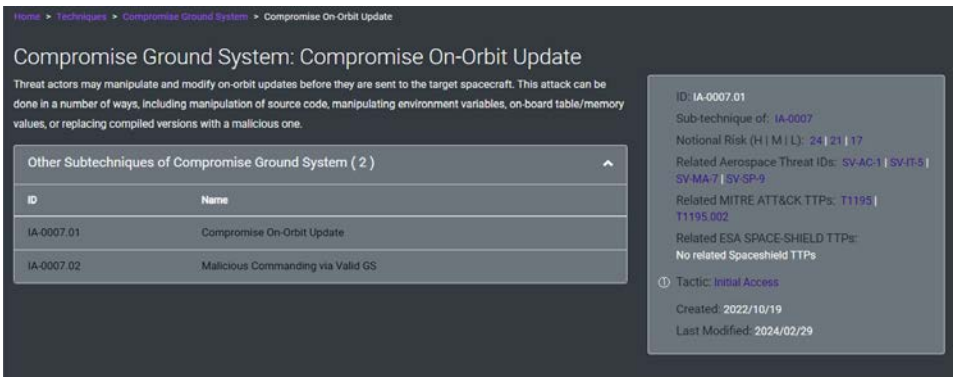


Figure 7. Compromised Ground System Technique and Subtechniques *(Source: SPARTA [14])*.

involved a foreign threat actor gaining access to Goddard Space Flight Center using social engineering techniques, combined with an inadequately configured file transfer protocol server. The threat actor was able to access the server that contained RoSat flight mission files. Unbeknownst to the RoSat mission team, the threat actor changed values in the algorithms used by the system's star tracker, thus making it point toward the sun and overheating. The team was able to identify the issue and correct the satellite's positioning for what they thought was an accident, without knowing it was the result of cyber activities.

The foreign threat actor tried again months later—this time, changing the code for the altitude-control system. The satellite slewed out of control, pointing the X-ray imager toward the sun and irreparably damaging it completely [17].

Commercial Internet Service Provider Attack

On February 24, 2022, a multifaceted and deliberate cyberattack against a satellite network resulted in a partial interruption of the popular consumer-oriented satellite broadband server Viasat [18]. The cyberattack impacted several thousand customers and tens of thousands of other fixed broadband customers across Europe. Ultimately, tens of thousands of modems that were previously online and active dropped off the network.

Subsequent investigation and forensic analysis identified a ground-based network intrusion by an attacker exploiting a misconfiguration in a virtual private network appliance to gain remote access to the trusted management segment of the satellite network. The attacker moved laterally through the trusted management network to a specific network segment

used to manage and operate the satellites and then used the network's access to execute legitimate, targeted management commands on many residential modems simultaneously.

Juliana Suess, a research analyst and policy lead on space security at the defense think tank at the Royal United Services Institute, believes the cyberattack against the Viasat satellite system is a wake-up call to the space industry [12]. The European Union, United Kingdom, and United States have linked the attack to Russia, prompting the U.S. National Security Agency to speak out about satellite security.

CONCLUSIONS

Cybersecurity in LEO satellite systems presents unique challenges and opportunities due to the specific characteristics of their orbits. The cyberspace landscape for LEO satellites is multifaceted, encompassing traditional cyberthreats such as unauthorized access, data interception, and denial-of-service attacks, together with satellite-specific vulnerabilities.

A fundamental challenge in LEO cybersecurity is managing its vast satellite constellations, where the sheer volume of satellites exponentially increases the attack surface and thereby amplifies the complexity of securing its network. Each satellite represents a potential vulnerability,

Cybersecurity in LEO satellite systems presents unique challenges and opportunities due to the specific characteristics of their orbits.

underscoring the need for advanced authentication protocols and stringent data integrity safeguards across the entire constellation.

There is significant future potential in incorporating physical layer security methodologies and quantum cryptography for ultrasecure communication protocols and harnessing artificial intelligence for autonomous threat detection and mitigation. However, integrating such advanced technologies must be carefully calibrated to align with the inherent limitations of satellite systems, including power consumption, payload capacity, and computational constraints. Collaborative endeavors between satellite operators, cybersecurity professionals, and international regulatory organizations are critical in formulating comprehensive standards and frameworks that safeguard these assets while promoting continued innovation.

The security of LEO satellite systems will significantly influence their viability and reliability in delivering global connectivity, making it imperative to continually evolve cybersecurity strategies in this dynamic space environment. Lessons must be drawn from past cybersecurity incidents to shape a cyberspace future that is secure and resilient. ■

REFERENCES

[1] Saliby, C. "Classification of Satellite Orbits." Infographic using *Draw.io*, 2024.

[2] ESA. "Types of Orbits." https://www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits, accessed on 21 September 2024.

[3] Space.com. "Starlink Satellites: Facts, Tracking and Impact on Astronomy." https://www.space.com/spacex-starlink-satellites.html, accessed on 13 September 2024.

[4] Langbroek, M. "SpaceX Starlink Objects Train." SatTrackCam Leiden (b)log, https://sattrackcam.blogspot.com/2019/05/wowowow-spectacular-view-of-spacex.html, Screenshot, 29 May 2019.

[5] National Aeronautics and Space Administration (NASA). "What Are SmallSats and CubeSats?" https://www.nasa.gov/what-are-smallsats-and-cubesats, accessed on 12 September 2024.

[6] CubeSat. "CubeSat Design Specification." Rev. 14.1, CP-CDS-R14.1, CubeSat Program, Cal Poly, San Luis Obispo, CA, February 2022.

[7] Johnson, N. L. "Medium Earth Orbits." IAC-10-A6.4.1, NASA, 2010.

[8] NASA Science. "GOES Satellite Network." https://science.nasa.gov/mission/goes/, accessed on 22 September 2024.

[9] Oakley, J. "Protecting the Final Frontier." Apress, 2020.

[10] NASA Earth Science Data Systems. "Remote Sensing." https://www.earthdata.nasa.gov/learn/backgrounders/remote-sensing, accessed on 20 September 2024.

[11] Britannica. "Kármán Line." https://www.britannica.com/science/Karman-line, accessed on 18 September 2024.

[12] Wired. "Satellites Are Rife With Basic Security Flaws." https://www.wired.com/story/satellites-basic-security-flaws/, accessed on 28 September 2024.

[13] Straka, B. "Implementing a Microcontroller Watchdog With a Field-Programmable Gate Array (FPGA)." KSC-2013-091, Kennedy Space Center, April 2013.

[14] SPARTA. "Space Attack Research and Tactic Analysis." Countermeasure – Update Software, https://sparta.aerospace.org/countermeasures/CM0010, accessed on 18 September 2024.

[15] NASA. "State-of-the-Art of Small Spacecraft Technology." https://www.nasa.gov/smallsat-institute/sst-soa/deorbit-systems/, accessed on 20 September 2024.

[16] SPARTA. "Space Attack Research and Tactic Analysis (SPARTA)." Matrix, https://sparta.aerospace.org, accessed on 10 September 2024.

[17] U.S. Naval Institute. "ASAT Goes Cyber." https://www.usni.org/magazines/proceedings/2021/february/asat-goes-cyber, accessed on 15 September 2024.

[18] Viasat. "KA-SAT Network Cyber Attack Overview." https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview, accessed on 16 September 2024.

BIOGRAPHY

CHADI SALIBY is an accredited cybersecurity architect and established cybersecurity strategist and leader who designs and engineers complex Cloud and hybrid cyber solutions to include vulnerability and attack surface exposure assessment, incident response, cyber threat hunting and intelligence, and robust security frameworks and programs. He is the director of Cloud security for the APAC region in one of the largest SaaS banking providers and a subject matter expert for CompTIA and ISC2, where he collaborates with a large team of experts and professionals to develop and prepare a new generation of cybersecurity experts. Mr. Saliby graduated from the Centre International Des Sciences Technique in business computer and programming and continued his MBA Magister en Business et Administration at Sorbonne.

CSIAC Cybersecurity & Information Systems Information Analysis Center

TECHNICAL INQUIRY SERVICES

FOUR FREE HOURS

Research within our four focus areas available to academia, industry, and other government agencies. Log in to https://csiac.dtic.mil to submit your inquiry today.

TECHNICAL AREAS

Cybersecurity

Knowledge Management & Information Sharing

Modeling & Simulation

Software Data & Analysis

Photo Source: U.S. Air Force and 123RF.com

CS IAC JOURNAL

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) is a component of the U.S. Department of Defense's (DoD's) Information Analysis Center (IAC) enterprise, serving the defense enterprise of DoD and federal government users and their supporting academia and industry partners.

HTTPS://CSIAC.DTIC.MIL
CONNECT WITH US ON SOCIAL MEDIA.