Space System Cybersecurity
Space Industry Perspectives

January 2025

National Space Council
Office of the National Cyber Director
Executive Office of the President

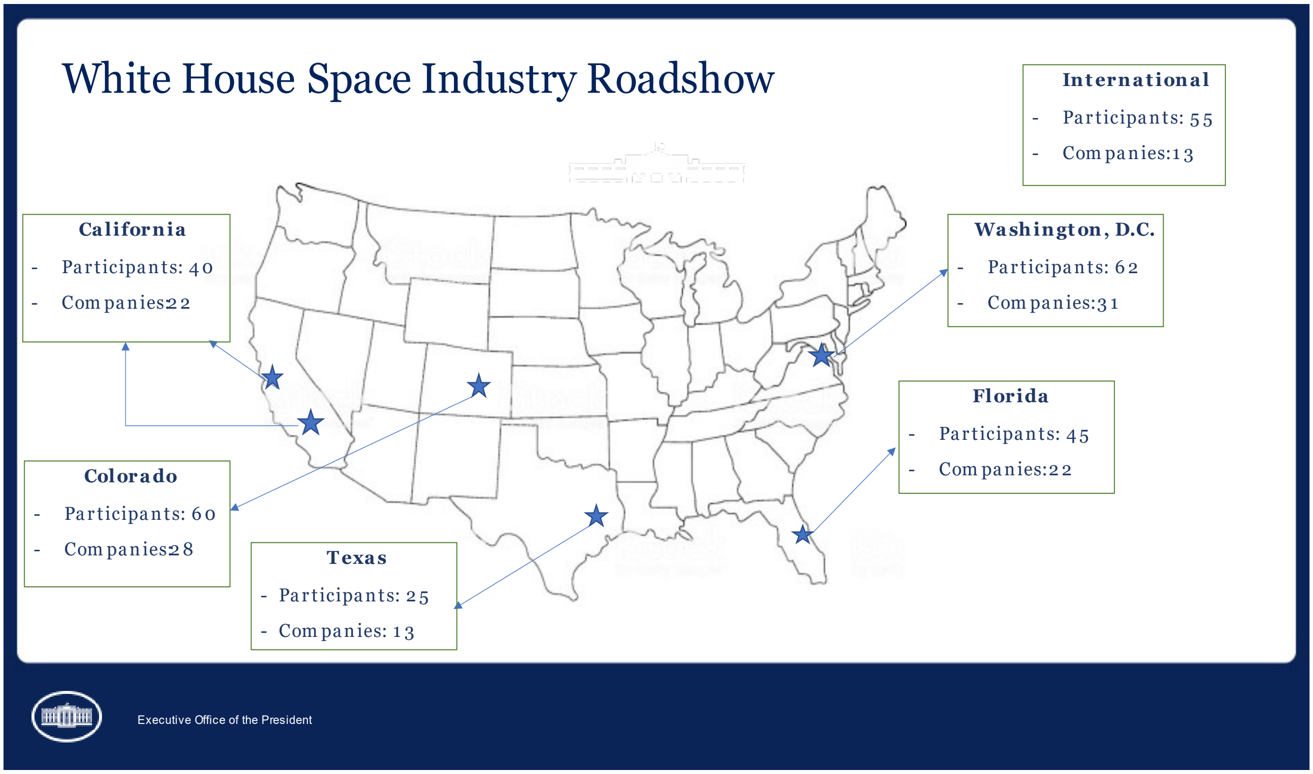
THE WHITE HOUSE
WASHINGTON

Table of Contents

Executive Summary

Today, space systems play an increasingly critical role for our national security, economy, and way of life. The global space economy was valued at USD $630 billion in 2023, with estimated growth to $1.8 trillion by 2035.[1] Growth in the U.S. space ecosystem has long been driven by government and established defense contractors. However, today, newer companies and investors are increasingly entering and diversifying the market, and commercial and government systems are more integrated than ever.

As the threat from malicious cyber actors to commercial and government space operators grows, it is critical that the U.S. Government understand private sector perspectives on ensuring secure and resilient space systems. Events preceding and following Russia's 2022 brutal and unprovoked war on Ukraine – including cyberattacks targeting private satellite companies – have only heightened the need to prioritize the cybersecurity of space systems, given their pivotal role underpinning global critical infrastructure and resilience.



White House Space Industry Roadshow

International
- Participants: 55
- Companies:13

California
- Participants: 40
- Companies22

Washington, D.C.
- Participants: 62
- Companies:31

Florida
- Participants: 45
- Companies:22

Colorado
- Participants: 60
- Companies28

Texas
- Participants: 25
- Companies: 13

Executive Office of the President

Given this changing economic and threat landscape – and, in alignment with the 2023 National Cybersecurity Strategy[2] – the White House began sustained engagement with U.S. space industry leaders in March 2023, at the Space System Cybersecurity Executive Forum. This event was designed to

[1] Space Economy Set to Triple to $1.8 Trillion by 2035, New Research Reveals > Press releases | World Economic Forum (weforum.org)

[2] The Biden-Harris Administration 2023 National Cybersecurity Strategy states, "the Administration remains committed to enhancing the security and resilience of U.S. space systems, including by implementing Space Policy Directive 5…"

facilitate robust discussion at the executive-level and motivate critical cybersecurity investments. White House staff then convened five working-level, technical workshops in key regional U.S. space industry hubs – California; Washington, D.C; Florida; Colorado, and Texas – to understand industry perspectives on space system cybersecurity best practices and identify gaps requiring White House and interagency action.[3] With the U.S. Department of State, the White House also held a roundtable for international space industry and governments to understand challenges among non-U.S.-based aerospace firms. Across these discussions, the White House engaged approximately 300 people representing 125 companies that span space mission areas.[4] During each half-day workshop, industry participants responded to a consistent question set focusing on two topics derived from Space Policy Directive (SPD)-5 – "Cybersecurity Principles for Space Systems" – cybersecurity-by-design and threat-informed operational practices to mitigate cyber risks.[5]

The following are the most common perspectives shared by space industry during discussions:

1. **Many perceive there is a highly-fragmented landscape of cybersecurity requirements for commercial and government-contracted space systems.** Many in space industry perceive inconsistency in government cybersecurity requirements, whether those related to the quality of code delivered, the feature set needed, or the manner in which the systems are operated. Currently, many companies develop their own internal cybersecurity quality requirements and feature sets in the product design phase based on interpretation of existing guidelines and frameworks.

2. **Many find cybersecurity operations technologies that can be deployed within the resource constrained, mission-critical requirements of space systems are lacking.** Many believe common terrestrial cyber-defense technologies, such as intrusion detection systems and sensors, do not have the appropriate level of accuracy, resource use, and maintenance specifications for space mission deployment and integration.

3. **Many believe existing U.S. Government cybersecurity operations guidelines and frameworks are broad and generally applicable to enterprise information technology (IT) cybersecurity, rather than space systems.** Many in space industry recognize unique characteristics of space systems in comparison to terrestrial critical infrastructure, as they encompass multiple, interconnected segments – user, ground, data/link, and on-orbit. Space industry broadly perceives existing voluntary government cybersecurity operations frameworks primarily provide guidance for terrestrial and traditional IT systems and generally do not assist in linking IT and operational technology (OT) systems.

4. **Many believe retroactively levying cybersecurity operations requirements on legacy space systems, or attempting to add cybersecurity features, would be too difficult.** Space and cyber experts broadly agree legacy space systems – many operating decades beyond expected design life – were generally built without cybersecurity in mind. Addressing security vulnerabilities in these legacy systems

[3] Readout of Space Systems Cybersecurity Executive Forum Hosted by the Office of the National Cyber Director and the National Space Council | The White House

[4] This number comprises primarily U.S.-owned space companies, as well as a smaller number international firms. Several companies sent representatives to more than one regional workshop. Companies represented the following elements of the industry: satellite communications; imagery/commercial remote sensing; launch; data/cloud services; large contractors; and, venture capital.

[5] See Addendum 2

would require government, not space industry, to develop unique solutions to ensure resilience to today's cyber threats.

5. **Many space industry cybersecurity experts perceive that their cyber and space missions are disconnected.** According to cybersecurity teams, space system development teams see cybersecurity as detracting from companies' core space mission development and as an impediment to technical innovations required for developing competitive and operationally-viable missions. In addition, the space industry is generally not motivated to make investments in new cybersecurity features or quality measures, including in light of perceived lack of customer demand. Many believe there must be a cultural shift to increase understanding that cybersecurity is fundamental to secure and resilient civil, commercial and defense space missions.

6. **Many believe baseline cybersecurity operations hygiene can be improved through more accountability for compliance with defined cybersecurity guidelines for space systems.** Broadly, space industry reported voluntary guidelines do not motivate companies to invest in minimum cybersecurity requirements for their space missions. Many raised regulation, updated policy with 'teeth,' and incentives and disincentives as mechanisms to ensure improved practices across the space industry.

7. **Many believe the space industry dedicates more time and resources to compliance, and translating existing requirements, than on actively developing and implementing cybersecurity operations best-practices.** Many space industry representatives noted the significant time and resources they spend understanding and complying with a broad range of cybersecurity frameworks that may or may not be directly applicable to space systems. The space industry broadly sees compliance activities as detracting from productive activities to mitigate cyber threats and vulnerabilities, including table-top exercises and penetration testing.

8. **Many believe information on space cyber threats is inconsistent, untimely, not actionable, lacking context and, in some cases, overclassified.** A large number of space companies reported widely varying access to cyber threat information, including from U.S. government, private sector, and open-source entities. Larger and smaller space companies reported clear disparities in access. When threat intelligence is received, space industry shared it is not always useful for driving concrete action.

9. **Many believe space startups have an advantage in incorporating better cybersecurity quality principles, as they are smaller and more agile; however, some smaller firms perceive a resource trade-off between space mission objectives and cybersecurity.** Smaller companies expressed they are more likely to adopt modern approaches to cybersecurity *quality* when developing space systems, including use of secure software languages. However, implementing cybersecurity features may be more challenging given a perceived trade-off between achieving the fundamentals of space missions to maintain funding, and cybersecurity. Some noted that demonstrating viability to investors is the primary motivation in product design or operations, rather than prioritizing cybersecurity, except as required by government or commercial customer contracts. Further, some smaller firms may have less awareness of cyber threats and vulnerabilities in the system design phase.

10. **Many are concerned about software and technology supply chain risk management, including at the subcontractor level.** Space industry prime contractors expressed consistent concern with lack of visibility into supply chain risks that could be introduced by subcontractors, while acknowledging that oftentimes larger companies do not communicate clear cybersecurity requirements downstream. Large

and small firms broadly identified a lack of guidance for understanding cyber risks when integrating components and tools from multiple vendors.

11. **Many believe expertise at the intersection of aerospace and computer engineering, as well as other relevant disciplines, is lacking across industry and government workforces.** Space industry representatives broadly perceive there is a limited workforce with cross-cutting expertise in computer science and aerospace engineering to ensure cybersecurity features are incorporated into space missions by design. Academic institutions and companies acknowledged a clear need to introduce students to cybersecurity principles early on and emphasize real-world application to interdisciplinary problems, including within the space ecosystem.

Background and Context

In light of opportunities provided by the growth of the commercial space ecosystem, persistent cyber threats to space systems present an urgent challenge. However, space systems present unique obstacles from a cybersecurity standpoint. These obstacles include lack of physical accessibility post-launch, which limits many methods of failure mitigation; limited size, weight and power (SWAP) capacity; expansive risk profile across nation-state borders; and, systems' dual-use civilian and military nature. The U.S. government has made significant progress in developing cybersecurity standards for terrestrial critical infrastructure sectors, but holistic space cybersecurity practices are underdeveloped. Early discussions with U.S. government and space industry executives led the White House to prioritize building on existing national policy, including Space Policy Directive-5, "Cybersecurity Principles for Space Systems," to mitigate cybersecurity vulnerabilities and address cyber threats. These discussions emphasized the need for tangible, comprehensive guidance for government and commercial space system developers and operators to measurably improve the cybersecurity of their space systems in the current threat environment.[6]

Throughout the Technical Workshop series, the White House received feedback on a range of cybersecurity frameworks and requirements broadly applicable to space systems. Many apply to the security of space systems, while several pertain to cybersecurity of enterprise systems used in the design, development, and manufacture of space systems. Additionally, the White House observed that remarks about cybersecurity frameworks applicable to space systems often did not differentiate between requirements in the design phase (i.e., when designing and building a satellite) and those in the operational phase (i.e., keeping the system secure once on-orbit). To help disambiguate across these distinct, but related, applications of cybersecurity frameworks and requirements, this report uses the following taxonomy to categorize key takeaways from the space industry discussions:

- Cybersecurity Quality – requirements associated with the underlying code itself are part of the *quality* control associated with a space system. For instance, there may be requirements that a codebase be written in a type-safe language, or use a set of compiler flags that reduce the chance of unintentional bugs that can be exploited. Fundamentally, *quality* choices are about reducing vulnerabilities in the code (as opposed to those due to insecure or unsecure configurations).

- Cybersecurity Features – requirements for specific cybersecurity functionality are part of *feature* choices tied to a space system. Capabilities for encryption or logging are both examples of cybersecurity *features* that may be required by contract. Implementation of *features* is still subject to quality challenges – as an example, cybersecurity operators might implement logging in a way that unintentionally allows for exploitation.

- Cybersecurity Operations – requirements levied on entities making use of space systems are *operational* in nature. These might include configuration requirements regarding use of multifactor authentication or management requirements, such as length of time logs must be retained.

[6] Readout of Space Systems Cybersecurity Executive Forum Hosted by the Office of the National Cyber Director and the National Space Council | The White House

Cybersecurity *operations* requirements may also be passed to contractors designing and building space systems; however, these requirements apply to information and communications technology (ICTS) used to design and develop the space systems, not the space systems themselves.

Space industry participants in each of the five U.S. workshops, as well as the international industry and government roundtable, were aware their insights would be utilized to inform U.S. Government policy.

Space System Cybersecurity: Summary of Space Industry Perspectives

1. **Many perceive there is a highly-fragmented landscape of cybersecurity requirements for commercial and government-contracted space systems.** Many in space industry perceive inconsistency in government cybersecurity requirements, whether those related to the quality of code delivered, the feature set needed, or the manner in which the systems are operated. Currently, many companies develop their own internal cybersecurity quality requirements and feature sets in the product design phase based on interpretation of existing guidelines and frameworks.

   Consistently, space industry experts expressed frustration with the wide range of cybersecurity requirements for space systems today – relevant to quality, features, and operations – leading industry to prioritize other factors, such as cost and schedule. Existing requirements related to enterprise cybersecurity are often difficult to translate and/or not easily applicable. From companies' perspectives, each individual government customer has different cybersecurity requirements, which may or may not be reflected in contract language.

   Regarding space system design, some companies believed the most effective way to ensure cybersecurity is baked in is for government to specify and build quality and feature requirements into government processes – including acquisitions rules and contract language – while accounting for cost. However, other companies were wary overly specific requirements for the unique space systems ecosystem could slow design and delivery and drive-up costs.

   As commercial and government systems are increasingly integrated, some companies noted U.S. cybersecurity requirements for commercial and government, civil, and national security systems should be consistent. Others expressed interest in moving toward common international cybersecurity technical standards for space systems.

2. **Many find cybersecurity products that can be deployed operationally within the resource constrained, mission-critical requirements of space systems are lacking.** Many believe common terrestrial cyber-defense technologies, such as intrusion detection systems and sensors, do not have the appropriate level of accuracy, resource use, and maintenance specifications for space mission deployment and integration.

   On many occasions, industry representatives expressed that large elements of the space systems ecosystem operate without cybersecurity sensors tailored for the on-orbit environment. Currently, companies instead rely on anomaly detection in telemetry streams to attempt to detect threats. They acknowledge that developing lightweight sensors – suitable for the resource-constrained on-orbit environment – would require significant research and funding to achieve. Some space industry representatives questioned the viable options, while others suggested government could consider future design standards or feature requirements to ensure cybersecurity sensors are incorporated.

3. **Many believe existing U.S. Government cybersecurity operations guidelines and frameworks are broad and generally applicable to enterprise information technology cybersecurity, rather than space systems.** Many in the space industry recognize the unique characteristics of space systems compared to terrestrial critical infrastructure, as they encompass multiple, interconnected segments – user, ground, data/link, and on-orbit. Space industry broadly perceives that existing voluntary

cybersecurity operations frameworks primarily provide guidance for terrestrial and traditional IT systems and generally do not assist in linking IT and OT systems.

Broadly, the space industry representatives perceived there are a number of U.S. government cybersecurity control sets for terrestrial systems and that these generally lack application to space systems on-orbit. Industry representatives shared that companies often need to 'cross-walk' existing guidance and figure out how to apply cybersecurity controls for IT and OT systems to the space vehicle. Smaller companies further struggle to prioritize which government-issued guidance to follow.

Given the wide range of voluntary standards that must be tracked, the space industry resoundingly agrees the U.S. Government should promote common cybersecurity *quality* and *feature* requirements for space systems and incorporate these in acquisitions and contract language. Industry was near-unanimous that rather than creating more standards, *harmonization* and *identification of minimum cyber standards* for space systems are sorely needed. In the absence of harmonized or minimum standards, space companies use their own internal processes to develop cybersecurity controls to address risk from nation-state cyber threats.

4. **Many believe retroactively levying cybersecurity operations requirements on legacy space systems, or attempting to add cybersecurity features to them, would be too difficult.** Space and cyber experts broadly agree that legacy space systems – many operating decades beyond expected design life **–** were generally built without cybersecurity in mind. Addressing security vulnerabilities in these legacy systems would require government, not space industry, to help develop unique solutions to ensure resilience to today's cyber threats. Legacy space systems present unique challenges from a cybersecurity standpoint. The industry broadly understands cybersecurity must be considered for legacy systems to be brought into modern space architectures, but doing so would require significant investment that many are resistant to commit to across the ecosystem. Many companies emphasized that on-orbit systems lack sensor data, and thinking on indications and warnings (I&W) for cyberattacks in space is largely undeveloped. These legacy systems use legacy coding languages (including C and C++), which in turn drives the continued use of these languages across the industry, despite known vulnerabilities. Some companies requested government consider exceptions or waivers to any policy shifts requiring use of specific languages, to account for legacy systems and many integrated sub-systems.

   Given the significant cybersecurity challenge posed by legacy space systems, representatives broadly recommended government take a forward-focused, rather than retroactive, approach to space system cybersecurity requirements.

5. **Many space industry cybersecurity experts perceive that their cyber and space missions are disconnected.** According to cybersecurity teams, space system development teams see cybersecurity as detracting from companies' core space missions and an impediment to technical innovations required for fielding competitive and operationally-viable products and services. In addition, space industry is generally not motivated to make investments in new cybersecurity features or quality measures, including in light of perceived lack of customer demand. Many believe there must be a cultural shift to increase understanding that cybersecurity is fundamental to secure and resilient civil, commercial, and defense space missions.

Space companies generally see cybersecurity as a constraint on space program delivery. From executives to program managers, cybersecurity is often considered a cost that detracts from companies' primary space missions during the design and delivery phase. Some believe this is because traditional aerospace engineers do not sufficiently understand cyber threats and mitigations, and because organizations silo aerospace and computer engineering workforces, preventing collaboration on cross-cutting challenges like space system cybersecurity.

Companies provided several recommendations to address a perceived lack of common mission across the space industry. Human spaceflight companies suggested 'safety' as a unifying metric to galvanize space program managers to prioritize cybersecurity. Others suggested providing regular threat briefs to aerospace and computer engineering employees to educate them on how cybersecurity ensures resilience of all space missions supporting civilians and the warfighter. Others suggested physically co-locating aerospace and computer engineers to increase mutual understanding – including regarding how cybersecurity fits in context of size, weight and power constraints for space systems. Resoundingly, the industry emphasized the need for space missions to account for cybersecurity (including implementing Development, Security and Operations – DevSecOps – principles) from the start as missions are designed.

6. **Many believe baseline cybersecurity operations hygiene can be improved through more accountability for compliance with defined cybersecurity guidelines for space systems.** Broadly, space industry reported voluntary guidelines do not motivate companies to invest in minimum cybersecurity for their space missions. Industry raised regulation, updated policy with 'teeth,' and incentives and disincentives as mechanisms to ensure improved practices across space industry.

   In discussing potential motivating factors, some industry participants referred to Pillar 3 of the Biden-Harris Administration National Cybersecurity Strategy – which emphasizes shaping market forces in favor of improved cybersecurity outcomes – as a framework for incentivizing cybersecurity investments for commercial space systems. Many noted that today, companies can choose whether or not to spend on cybersecurity, and need accountability for maintaining a minimum threshold.

   Some companies raised cyber insurance as a unique challenge for the space industry, as insurers often do not understand specific threats to space system owners and operators, making it difficult to validate risks.

7. **Many believe space industry dedicates more time and resources to compliance, and translating existing requirements, than on actively developing and implementing cybersecurity operations best-practices.** Many space industry representatives expressed frustration regarding the significant time and resources they spend understanding and complying with a broad range of cybersecurity frameworks that may or may not be directly applicable to space systems. Space industry broadly sees compliance activities as detracting from productive activities to mitigate cyber threats and vulnerabilities, including table-top exercises and penetration testing.

   Many companies have staff dedicated to tracking and translating the wide range of U.S. government and international cybersecurity standards applicable to space systems. Some raised the significant amount of industry overhead dedicated to compliance with standards. Companies see a clear trade-off in time spent on compliance, vice practicing activities that tangibly increase resilience to malicious cyber operations.

Companies expressed a preference to spend time and resources on activities like table-top exercises using real-world scenarios with engineers, developing strong penetration testing skills for space vehicles, or thinking beyond static requirements toward continuous system monitoring and maintenance post-launch.

8. **Many believe information on space cyber threats is inconsistent, untimely, not actionable, lacking context and, in many cases, overclassified. Space companies reported widely varying access to cyber threat information, including from a large number of U.S. government, private sector, and open-source entities.** Larger and smaller space companies reported clear disparities in access. When threat intelligence is received, space industry shared it is not always useful for driving concrete action.

   Larger and medium-sized space companies generally reported they regularly receive cyber threat information from a range of U.S. government intelligence agencies and commercial sources. However, some did not understand U.S. intelligence agencies' differing roles and responsibilities, and reported receiving threat intelligence from multiple agencies. Most companies recognize the importance of tracking threats and noted the temporal element is critical for space systems – operators need to understand threats to legacy, current, and future space missions simultaneously.

   Most companies believe the U.S. government can better distill threat intelligence in ways that provide context, make it actionable, and include impact analysis. Companies expressed interest in more information on likely attack vectors, as well as threats to on-orbit systems.

   Companies believe two-way information sharing is critical. Industry concerns about shareholder and investor views, and the competitive nature of the space economy, may disincentivize information sharing with government in some cases. Outside government channels, companies do leverage commercial to commercial information sharing networks, and some firms have bilateral agreements that facilitate effective sharing.

9. **Many believe space startups have an advantage in incorporating better cybersecurity quality principles, as they are smaller and more agile; however, smaller firms often perceive a resource trade-off between space mission objectives and cybersecurity.** Smaller companies expressed they are more likely to adopt modern approaches to cybersecurity *quality* when developing space systems, including use of secure software languages. However, implementing cybersecurity *features* may be more challenging given a perceived trade-off between achieving the fundamentals of space missions to maintain funding and cybersecurity. Some noted that demonstrating viability to investors is the primary motivation in product design or operations, rather than prioritizing cybersecurity, except as required by government or commercial customer contracts. Further, some smaller firms may have less awareness of cyber threats and vulnerabilities during system design.

   Some companies believe the increased commercialization of space has introduced more security, and cybersecurity-by-design is well understood, if unevenly implemented. These companies consider the relative speed of industry innovation an advantage in implementing cybersecurity design principles more quickly if small companies are engaged early on.

Other small firms stated cost is the motivating factor in the system design phase. These companies' primary focus is demonstrating viability to investors – rather than prioritizing cybersecurity in product design or operations – except as required by government or commercial customer contracts. Further, smaller space firms are not uniformly aware of cyber threats and vulnerabilities in the system design phase or the connection between product security and business viability. Broadly, smaller firms expressed a need for flexibility and recognition by government that cost is top of mind and a clear demand signal for minimum cybersecurity requirements is needed.

10. **Many are concerned about software and technology supply chain risk management, including at the subcontractor level.** Prime contractors expressed consistent concern with lack of visibility into supply chain risks upstream, while acknowledging larger companies can do better to communicate clear cybersecurity requirements.
    Prime contractors generally believe government must institute clear guidance on cybersecurity design elements and cybersecurity operations controls, paired with incentives, to ensure upstream resilience, including for second- and third-tier suppliers. Both larger and smaller space firms recognize if minimum cybersecurity requirements are not built into government contract requirements, firms will largely not implement them consistently.

11. **Many believe expertise at the intersection of aerospace and computer engineering, as well as other relevant disciplines, is lacking across industry and government workforces.** Space industry broadly perceives there is a limited workforce with cross-cutting expertise in computer science and aerospace engineering to ensure cybersecurity features are incorporated into space missions by design. Academic institutions and companies acknowledged a clear need to introduce students to cybersecurity principles early on and emphasize real-world application to interdisciplinary problems, including within the space ecosystem.

    Broadly, space companies recognize the entire workforce must be bought-in on cybersecurity. Across space industry, cybersecurity is most challenging at the space vehicle level; today, there is not a robust industry workforce with knowledge of existing cybersecurity standards or nation-state threats. As the space environment is unique, such interdisciplinary skills often must be learned on the job.

    Academic institutions and companies acknowledged a clear need to introduce students with diverse backgrounds and skillsets to cybersecurity principles early in their education, and to emphasize cybersecurity should not be considered in a vacuum but applied to real-world challenges. Global competitions like Hack-A-Sat demonstrate strong interest in the emerging field of penetration testing active space vehicles. Industry and academic representatives noted such programs can help get students interested in technical, interdisciplinary topics in high school, college and non-traditional learning settings.

ADDENDUM 1: List of Participant Entities in White House Space System Cybersecurity Technical Workshops (U.S. and International)

- Aerospace Corporation
- Air Force Research Laboratory
- Amazon Project Kuiper
- Amazon Web Services
- Applied Tech
- Arlington Chamber of Commerce
- Astroscale US
- Axiom Space Inc.
- BAE Systems Digital Intelligence
- Belcan
- BlackSky Holdings, Inc.
- Blue Origin
- Booz Allen Hamilton
- BRPH Architects Engineers Inc
- Canadian Space Agency
- Capella Space
- Center for the Study of the Presidency & Congress
- City of Los Angeles
- Collins Aerospace
- Colorado Chamber of Commerce and Economic Development Corporation
- Colorado Springs Black Chamber of Commerce
- Commercial Spaceflight Federation
- Cornell University
- Cromulence LLC
- Cyber Florida
- Deloitte
- Earth Observant Inc.
- Echostar
- EchoStar/Hughes
- Embassy of Finland
- Embassy of France
- Embassy of India
- European External Action Service
- European Space Agency
- Eutelsat SA
- Falcon ExoDynamics
- German Federal Office for Information Security (BSI)
- Florida Institute of Technology
- French National Cybersecurity Agency (ANSSI)
- General Dynamics Information Technology
- General Dynamics Mission Systems
- German Ministry of Interior (BMI)
- GLESEC
- Google
- Government of the United Kingdom
- GXO, Inc
- Hypersat
- Infosys
- Intuitive Machines
- Iridium
- Johns Hopkins Applied Physics Lab
- Kratos Defense and Security
- L3Harris Technologies
- Leidos
- Lockheed Martin
- Los Angeles Chamber of Commerce
- Lucid Circuit
- Luxembourg Embassy, Washington, D.C.
- Mandiant/Google Public Sector
- Maryland Chamber of Commerce
- Maxar Technologies
- Microsoft
- MITRE
- Mitsubishi Corporation (Americas)
- Modern Technology Solutions, Inc.
- National Aeronautics and Space Administration (NASA)
    - Headquarters
    - Ames Research Center
    - Jet Propulsion Laboratory
    - Johnson Space Center

    - Kennedy Space Center
- National Geospatial-Intelligence Agency
- National Reconnaissance Office
- National Security Agency
- National Security Space Association
- National Technical Systems (NTS)
- NEC Corporation
- Northrop Grumman
- OneWeb
- Optus Satellite
- Orlando Economic Partnership
- Pacific Defense
- Palantir Technologies
- Parsons
- Peraton
- Planet Labs
- Purdue University
- Quindar
- Raytheon Technologies (RTX)
- Redwire Space
- Relativity Space
- Rocket Labs
- Safran Data Systems, Inc.
- Sigmatech
- Slingshot Aerospace
- Space Coast Black Chamber of Commerce
- Space Florida
- Space Information Sharing and Analysis Center
- Space Logistics
- Spaceit
- SpaceX
- SpiderOak
- Stellar Solutions Inc
- Stephenson Stellar Corp
- Stoke Space Technologies
- TechCentrics, Inc
- The Boeing Company
- True Anomaly
- U.S. Chamber of Commerce
- U.S. Department of Commerce/National Institutes of Standards and Technology (NIST)
- U.S. Department of Defense
- U.S. Department of Homeland Security
    - Cybersecurity and Infrastructure Security Agency (CISA)
    - Policy
- U.S. Department of Justice, Federal Bureau of Investigation (FBI)
- U.S. Department of State
- Umbra
- United Launch Alliance
- United States Department of Energy
- United States Space Force
- University of Central Florida
- University of Florida
- United States Space Command
- Viasat
- Virginia Department of Emergency Management
- Virginia Spaceport Authority
- Xage Security
- Xona Space

ADDENDUM 2: White House Space System Cybersecurity Technical Workshops: Template Agenda

Office of the National Cyber Director (ONCD)
Technical Workshop on Space System Cybersecurity

0800 – 0815: **Arrival and Light Refreshments**

0815 – 0825: **Welcome and Framing Remarks** *(ONCD)*

0825 – 0835: **Participant Introductions** *(All)*

0835 – 1005: **Session 1:** Cybersecurity-by-Design *(All)*

This session will focus on various practices industry is currently using to apply cybersecurity-by-design principles to protect space systems/assets from cybersecurity-related risks and vulnerabilities, in line with the principles set forth in Space Policy Directive-5 (SPD-5), "Cybersecurity Principles for Space Systems." This may include standards, guidelines, contract language, and other best-practices leveraged to manage cyber risk across the full lifecycle of space-related assets.

1005 – 1020: **Break**

1020 – 1150: **Session 2:** Operational Practices to Mitigate Cyber Risk *(All)*

This session will explore mechanisms industry is using to obtain and operationalize cyber threat information; common cyber incident response and management practices; and differences in how conventional enterprise cybersecurity activities (e.g., logging, network monitoring) are carried out on space systems. The session will also focus on limitations to cyber threat information sharing, in line with Space Policy Directive-5, and potential approaches for improvement.

1150 – 1205: **Break**

1205 – 1230: **Around-the-Room and Recap** *(All, ONCD)*

Office of the National Cyber Director (ONCD)
Technical Workshop on Space System Cybersecurity

Guiding Questions

Session 1: Cybersecurity-by-Design

1. Given the nexus between cybersecurity and traditional engineering disciplines, how does your company/organization bridge this issue in your complex environments? How do you think about cybersecurity beyond software and hardware?

2. What existing cybersecurity-specific processes and/or procedures do you leverage within your organization to understand cybersecurity vulnerabilities in your space systems and related assets? What are the key challenges you face in implementing cybersecurity at the systems level?

3. How do you balance cybersecurity guidelines and requirements with other organizational priorities, especially cost, during system design?

4. As you balance risk, innovation, and cost, do you leverage OpenAI technologies or off-the-shelf commercial products to drive product development? How do you ensure all stakeholders in your organization, including contractors and suppliers, comply with cybersecurity best practices, guidelines, and your cybersecurity requirements?

5. What challenges have you faced implementing cybersecurity measures for your space systems, and how have you addressed them?

6. What do you see as challenges when integrating cybersecurity assessment processes (e.g., pen-testing, red/purple teaming) with your existing systems-engineering verification and validation processes?

7. Are there technical or policy approaches that may improve or advance implementing cybersecurity-by-design?

Session 2: Operational Practices to Mitigate Cyber Risk

1. How does your organization address cybersecurity incidents or breaches that affect your space systems and related assets, including through the use of cyber insurance? From your organization's perspective, is there utility in government requirements for tools like cyber insurance?

2. In what ways do your enterprise-related cybersecurity risk management practices differ from, or complement, your space system-related cybersecurity?

3. How do you assess and manage threat-informed cybersecurity risks to your space systems and related assets?

4. How frequently are cyber-based threats assessed and reassessed that could potentially impact your company/organization? Do you develop and/or have resilience plans in place to address potential cybersecurity impacts?

5. In what ways does your organization collaborate across public and private sectors on threat information to develop and implement cybersecurity best practices? What limitations, if any, exist for you to be able to fulsomely act upon relevant cyber threat-related information?

6. In the National Cybersecurity Strategy, Objective 3.3 focuses on shifting liability for insecure software products and services. As part of this objective, the federal government is to invest in the development of secure software, including memory-safe languages (such as Rust). How has your company/organization thought through or implemented these kinds of objectives? What, if any, limitations exist?

7. What are challenges your workforce currently faces in ingesting and acting upon threat information?

8. As we think of the constantly evolving cyber threat landscape, how are you thinking of future resilience from cyber-based threats? What recommendations do you have for policy consideration?