CSC 2.0

April 2023

Time to Designate Space Systems as Critical Infrastructure

Frank Cilluffo
RADM (Ret.) Mark Montgomery
Sharon Cardash
Kelsey Shields

Table of Contents

Executive Summary

Today's space race features not only weapons systems but also satellites that provide global positioning, remote imagery, and communication services. These services are integral both to America's national security and to its economy.

"We're in a space race" with China, NASA Administrator Bill Nelson warned in December.[1] The nature of that race is different from the Cold War contest with the Soviet Union that America fought and won. The national security components of the space race today include not just weapons systems but also the security of critical infrastructure — much of which relies on global positioning satellites, remote imagery, and advanced communication. The economic aspect is just as striking. The Space Foundation, a nonprofit advocacy group, has determined that the global space industry generated $469 billion in revenue in 2021.[2] This number will only increase with technological and manufacturing innovation.

More than a decade ago, the U.S. National Security Space Strategy warned that space will become more "congested, contested, and competitive."[3] This warning proved prescient, but the U.S. government has not done enough to adapt to that reality. Major portions of American space systems are still not designated as critical infrastructure and do not receive the attention or resources such a designation would entail. The majority of today's space systems were developed under the premise that space was a sanctuary from conflict, but this is no longer the case. The threat from Russia and China is growing. Both those authoritarian powers have placed American and partner space systems in their crosshairs, as demonstrated by their testing of anti-satellite (ASAT) capabilities. The United States needs a more concerted and coherent approach to risk management and public-private collaboration regarding space systems infrastructure.

After interviewing more than 30 industry and government experts, the authors have concluded that designating space systems as a U.S. critical infrastructure sector would close current gaps and signal both at home and abroad that space security and resilience is a top priority. In 2013, Presidential Policy Directive-21 (PPD-21) designated 16 critical infrastructure sectors "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[4] Space systems clearly meet this threshold.

The term "space systems" encompasses the ecosystem from ground to orbit, including sensors and signals, data and payloads, and critical technologies and supply chains.[5] (See Figure 1.) This terminology (which sidesteps the conceptual debates about whether "space" is an infrastructure or only a domain)[6] aligns with presidential Space Policy Directive-5 (SPD-5) of September 2020, which defines space systems to include ground systems, sensor networks, and space vehicles.[7] SPD-5 provided a set of voluntary best practices "to guide and serve as the foundation for the United States Government approach to the cyber protection of space systems." This report seeks to build on these efforts, which constituted an important step toward recognizing and addressing the implications of the nexus between the cyber and space domains.

Protecting space systems will require an enhanced model of public-private partnership with genuinely shared risk management responsibilities. On the government side, the agency that serves as lead sector risk management agency (SRMA) for this sector will have a demanding task — but one that NASA is well suited to fulfill so long as it receives the extra resources necessary to develop its capacity to protect national security, civil, and commercial systems. There will need to be subgroups within the sector that maintain relationships with other government agencies. One subgroup should deal with defense and intelligence systems, and another with communications systems already regulated by the Federal Communications Commission (FCC). But no alternative candidate for lead SRMA possesses the same range of requisite capabilities as NASA.

Fostering security and resilience in the space systems sector will require mitigating unique cybersecurity challenges that stem from the geographic and technological particularities of space, as well as new and emerging space-based missions. Substantial investment through congressional appropriation will be imperative because policy without resources is merely rhetoric.

Recommendations Summary

For the Executive Branch

Recommendation 1: Designate space systems as a critical infrastructure sector.

1.1 – Designate NASA as the SRMA for the space systems sector.

1.2 – Create two directed subgroups within the sector.

1.3 – Do not assign the SRMA a regulatory role.

1.4 – Articulate and offer industry a clear value proposition.

1.5 – Strengthen international norms and standards.

1.6 – Integrate the National Space Council into the governance of the space systems sector.

For Congress

Recommendation 2: Give NASA, the lead SRMA, the resources to effectively accomplish the mission.

2.1 – Direct the Congressional Research Service to undertake a legislative review.

For Industry

Recommendation 3: Marshal and organize the commercial space community to play an instrumental role in governance.

3.1 – Establish a space systems sector coordinating council (SCC).

3.2 – Task the SCC, through its charter, with working to reduce risks to the security and resilience of the commercial space sector.

3.3 – Leverage and build upon the existing work of Information Sharing and Analysis Centers (ISACs), including the Space ISAC.

For Industry and Government Together

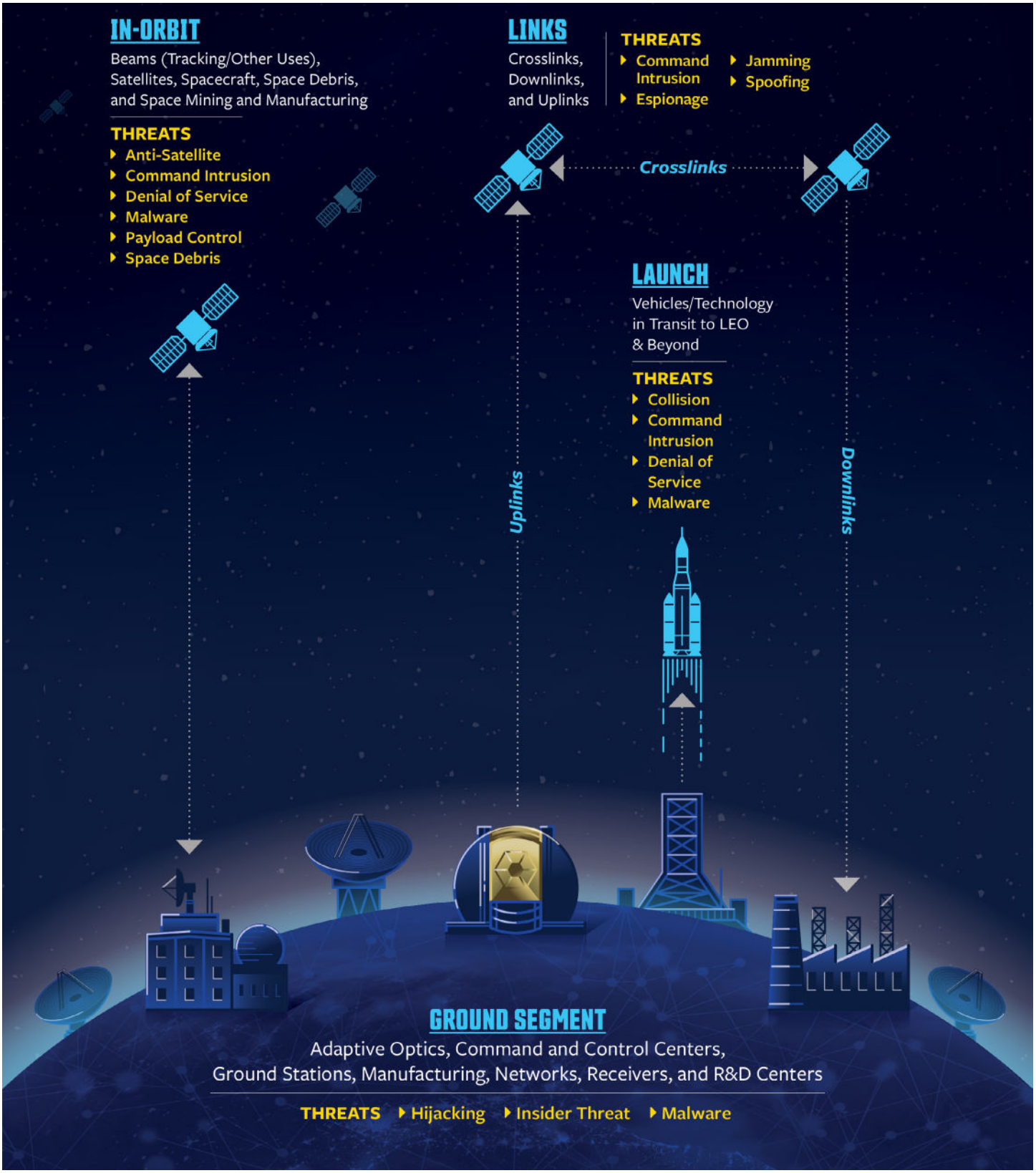
Recommendation 4: Create a co-led risk management enterprise.

4.1 – Jointly elaborate and widely implement cybersecurity best practices.

4.2 – Pair commercial and government capabilities to model a dynamic risk environment.

4.3 – Add space assets positioned outside of traditional operational areas to enhance U.S. resilience.

Figure 1: The space systems threat spectrum



The examples cited above are illustrative and not exhaustive.

Acronyms

Anti-Satellite	ASAT
Cybersecurity and Infrastructure Security Agency	CISA
Defense Industrial Base	DIB
Department of Defense	DoD
Department of Homeland Security	DHS
Electricity Sub-Sector Coordinating Council	ESCC
Federal Aviation Administration	FAA
Federal Communications Commission	FCC
Global Positioning System	GPS
Government Accountability Office	GAO
Government Coordinating Council	GCC
Information Sharing and Analysis Centers	ISACs
International Organization for Standardization	ISO
National Aeronautics and Space Administration	NASA
National Critical Functions	NCFs
National Defense Authorization Act	NDAA
Presidential Policy Directive-21	PPD-21
Sector Coordinating Council	SCC
Sector Risk Management Agency	SRMA
Space Information Sharing and Analysis Center	Space ISAC
Space Policy Directive-5	SPD-5

The Criticality of Space Systems and Threats to the Sector

Space systems serve fundamental roles in national security and economic prosperity and are at risk of disruption.[8] These risks stem from adversarial nations intent on causing harm to the United States and its partners and allies and are amplified by legacy technologies and the unique challenges of space.

Currently, space systems serve as the foundation for military operations, mission assurance, and intelligence, surveillance, and reconnaissance. Critical infrastructure sectors — energy and water, for example — rely heavily on satellites for positioning, navigation, and timing for industrial control systems that power pipelines and transmission lines.[9] Within the financial services sector, trading and transactions, ATMs, and credit cards all rely on space systems — as do the telecommunications, maritime transportation, and agricultural sectors. And in daily life, Americans rely on the global positioning system (GPS).

Meanwhile, the economic impact of space systems is growing rapidly, prompting at least one expert to suggest the economic dimension may soon equal and surpass the national security impact.[10] Estimates project that within 10 to 15 years, the value of the space industry could approach $1 trillion worldwide.[11] The Department of Commerce estimates that in 2019, the U.S. space economy generated $194.4 billion in real gross output — an increase of 20 percent from earlier in the decade, translating to 0.6 percent of U.S. gross domestic product.[12] During fiscal year 2021, NASA alone "generated a total economic output of more than $71.2 billion," according to the agency's October 2022 economic impact report.[13] The interplay between space and commerce will only expand as off-Earth manufacturing and mining mature and construction of commercial space

stations begins. Alongside these developments, soon-to-be-operational, fully reusable space launch systems made by SpaceX, Blue Origin, and others will have a transformative impact on space logistics and national defense.[14]

America's adversaries recognize the importance of space systems to U.S. national and economic security and have tested capabilities to destroy them.[15] In 2007 and 2021, respectively, China and Russia tested direct-ascent ASAT missiles. The Russian test alone created more than 1,500 pieces of debris big enough to track. Calling the test "dangerous and irresponsible," Secretary of State Antony Blinken warned the debris would "significantly" heighten the risk to the International Space Station.[16]

In February 2022, Moscow hacked U.S.-based satellite internet provider Viasat to disrupt Ukraine's military communications just an hour before Russia invaded the country.[17] The attack also disrupted internet service across Europe. Russia subsequently mounted electronic attacks, attempting to jam the Starlink constellation.[18] At a UN forum in October 2022, Russia asserted that commercial space systems "may become a legitimate target for retaliation."[19] A month later, U.S. government analysts revealed that they had discovered Russian state-backed hackers inside U.S. satellite communications networks, apparently operating undetected for months prior to discovery.[20]

China, for its part, has for years been honing the ability to strike enemy satellites using cyber operations, electronic warfare, and other means as part of the country's larger warfighting strategy and doctrine, designed to deny adversaries access to space-based systems.[21] A November 2022 Department of Defense (DoD) report on China's military capabilities warned that Beijing's civilian and military capabilities in space are rapidly maturing.[22] The report notes that the Chinese military is developing "kinetic-kill missiles, ground-based lasers, and orbiting space robots" as well as "satellite jammers; offensive cyberspace capabilities; and directed-energy weapons," which can not only monitor but also disrupt or destroy satellites.[23] The Pentagon further highlighted that Chinese military academics argue that attacks on satellites could "blind and deafen the enemy."[24] China is also copying SpaceX as fast as it can.[25]

Space systems are vulnerable to adversarial attacks for many of the same reasons as other critical systems. Adoption of cybersecurity best practices in the commercial space sector has been uneven, as satellites are typically designed for longevity, not security. Networks and technologies for controlling space assets may connect to corporate networks and the internet.[26] Adversaries may compromise increasingly complicated hardware and software supply chains. Communications between ground stations and satellites — known as uplinks and downlinks — are often transmitted through unencrypted or open networks and are thus susceptible to hostile intervention that could disrupt, degrade, or destroy data and operations and compromise vital missions.

Moreover, like all other critical infrastructure sectors, space systems use legacy technologies and protocols. Satellites may use old software that cannot be updated. They may not have the onboard processing required to update software. They may, due to construction constraints, lack redundancies that have become a standard best practice for resilience. While the situation regarding legacy technology in critical infrastructure is improving generally and within space systems in particular, space systems face the added difficulty that they must be repaired or replaced in orbit. The introduction of next-generation hardware and software only adds to the complexity.

Space systems also have unique physical and technical characteristics that result in additional risks. Space debris jeopardizes assets in orbit that serve vital national security and economic interests of the United States and its allies. Depending on the circumstances, the physical damage to critical infrastructure from severe weather or other natural disasters could potentially pale in comparison to the cascading failures that could result if debris hits a satellite and creates more debris. In 2021 and 2022, the International Space Station had to conduct emergency maneuvers to avoid space debris created by a Russian ASAT test.[27]

Space systems also lack so-called "compensating controls" — security measures that block physical proximity to sensitive systems. In space, few measures can prevent an adversary from positioning its satellite next to a U.S. satellite and electronically eavesdropping on American and allied communications. Space systems also often use specialized protocols — standards and rules for communicating information and transmitting data — that commercial off-the-shelf cyber-defense tools cannot monitor. Instead, specialized cyber sensors and tools are needed. These challenges, however, may diminish as systems

comprising handcrafted components give way to ones that employ mass-produced, reusable parts that can be manufactured quickly and relatively inexpensively.

Yet another feature of space systems that complicates risk management is that much of the U.S. terrestrial infrastructure is situated abroad. The United States does not launch all objects into space from U.S. territory.[28] For the purposes of risk management, most — but not all — of the infrastructure located elsewhere falls under the purview of DoD.

Government and Industry Steps to Change the Status Quo

The Biden administration, Congress, and the private sector have begun exploring ways to address the challenges outlined above. In May 2021, the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security announced the creation of a Space Systems Critical Infrastructure Working Group. The body aims to bring government and industry together to "identify and offer solutions to areas that need improvement in both the government and private sectors" and to "develop recommendations to effectively manage risk to space based assets and critical functions."[29] Members include representatives of the "communications, critical manufacturing, defense industrial base, information technology, and transportation sectors, including leading-edge satellite and space asset infrastructure firms with expertise in emerging technology areas." To date, the group has maintained a low public profile, making it difficult to assess the nature or impact of its work.

In tandem, as part of a broader statutory requirement in the National Defense Authorization Act (NDAA) for Fiscal Year 2021, CISA reviewed the current framework for securing critical infrastructure, the list of critical infrastructure sectors, and the designations of SRMAs.[30] The resulting report, reviewed and endorsed by President Joe Biden,[31] noted that CISA will "evaluate the establishment of the Space Sector as a critical infrastructure sector" based on the following criteria:

> "1. Does the scope describe a logical collection of assets, systems, or networks?
>
> 2. Does the scope provide common function to the economy, government, or society?
>
> 3. Could disruptions to the critical infrastructure sector lead to debilitating impacts on security, national economic security, national public heath, or safety?
>
> 4. Is the critical infrastructure sector subject to risk drivers not fully addressed through existing mechanisms, policies, or governance structures?
>
> 5. Do key stakeholders within the critical infrastructure sector need to actively maintain their partnership beyond any existing collaboration mechanisms that may be in place?"[32]

Each of these questions may be answered squarely in the affirmative. When releasing the report in November 2022, CISA noted that it will use the above criteria and collaborate with interagency partners "to evaluate the list of sectors and SRMAs through a phased approach to validate and refine the activities of the current sector structure."[33] In the National Cybersecurity Strategy, released in March 2023, the administration also committed to "enhancing the security and resilience of U.S. space systems."[34] A forward-leaning posture regarding space systems — that takes into account the coming of ubiquitous space operations and routine human and robotic spaceflight — will put the country firmly on the path to continued leadership in the 21st century.

In addition, within the Executive Office of the President, the National Space Council advises on "the formulation and implementation of space policy and strategy." The council's work spans the civil, commercial, and national security space.[35] The council is currently considering how to structure oversight of emerging on-orbit activities, such as servicing satellites,[36] and hosted the Space Systems Cybersecurity Executive Forum in conjunction with the Office of the National Cyber Director at the end of March.[37] To date, however, the council has not had the benefit of a partner in the form of a lead government agency or SRMA for space systems. The result is that policy and strategy have been promulgated at a certain level, removed from the operators that take the lead on implementation. Consequently, high-level guidance on sectoral priorities is not as deeply integrated as it could be, resource allocation is not optimized, and the government's overall effort is not as coherent

or effective as it should be. Revising the current sector structure to include a space systems sector would help to address these shortcomings.

Some lawmakers have also weighed in on how best to protect space infrastructure. Senators Gary Peters (D-MI) and John Cornyn (R-TX) introduced the Satellite Cybersecurity Act during the previous Congress.[38] If reintroduced and passed, this bipartisan bill would direct CISA to "develop voluntary satellite cybersecurity recommendations to help companies understand how to best secure their systems."[39] In June 2021, Representatives Ted Lieu (D-CA) and Ken Calvert (R-CA) introduced the Space Infrastructure Act, which would have designated "space systems, services, and technology as a critical infrastructure sector."[40] Also notable is section 1613 of the FY2021 NDAA, which requires the government to produce a "strategy to strengthen civil and national security capabilities and operations in space." Section 1614 mandates a "report and strategy on space competition with China."[41]

Meanwhile, the private sector has initiated its own efforts to remedy some shortcomings. The Space ISAC, which is industry-led and was created in 2019, is setting up a watch center whose initial operating capability is designed to foster not just a bilateral (public-private cross-sector) flow of information, but a multilateral flow that integrates partners worldwide. The Space ISAC is also setting up a cyber vulnerability lab to test hardware and software, with the aim of putting into place "a community expectation for cybersecurity for commercial space systems."[42] These and other industry-led efforts are undoubtedly valuable, but membership in the Space ISAC is voluntary and government initiative is required, for example, to amplify and implement the results of research and development and vulnerability testing for the protection of space systems.

The Necessity of a New Approach to Safeguarding Space Systems

Against the backdrop of rising threats, the U.S. government's current approach to safeguarding space and working with private industry to secure critical systems is insufficient. While pieces of the industry fall under communications infrastructure or the defense industrial base (DIB), too much is left uncovered. Recent government efforts to rectify the problem are promising but remain in their infancy. While not without its challenges, designating space systems as a critical infrastructure sector would begin to rectify these problems.

The authors interviewed more than 30 subject matter experts on a not-for-attribution basis, including current and former U.S. government officials and senior corporate executives. Experts from the national security (intelligence and homeland security), national defense, civilian space, and commercial space communities offered an array of recommendations on how best to support critical space systems.[43] The appendix lists the names of experts who agreed to be listed, but their inclusion does not imply that they or any organizations with which they are affiliated endorse the recommendations in this paper. While all interviewees affirmed the importance of space systems and recognized shortcomings in the current approach, there were differences of opinion on the solution. The authors' assessment, however, is that the balance of the arguments supports designation.

Experts in favor of retaining the status quo tend to have a minimalist view of the elements that fall outside the current sector structure, believing they are not yet sufficiently critical to warrant a new sector designation. Components of some space systems are currently designated as critical infrastructure within the framework of other critical infrastructure sectors.[44] Commercial communications satellites are considered part of the communications sector,[45] while military reconnaissance satellites and GPS systems are part of the DIB.[46] Meanwhile, the critical manufacturing sector includes aerospace parts and manufacturing, while the Federal Aviation Administration governs launch and re-entry from space as part of the transportation sector.

However, important components of space systems (particularly those operated by commercial remote sensing enterprises) are not represented in any critical infrastructure sector. Some satellites — particularly those used for scientific and other research purposes, including weather tracking and forecasting systems — are not part of either the communication or the DIB sectors, which could also soon be true of other emerging space-based systems for transportation, remote sensing, manufacturing, mining, and cislunar operations. The systems that launch and operate communications and other satellites, as well as "the companies that manufacture, launch, or operate space vehicles or the supply chains that sustain all these

systems," are also not represented in the current framework governing critical infrastructure sectors, according to the industry-led group, the Space ISAC.[47]

With space commerce set to expand, the argument that only marginal activities remain outside current critical infrastructure designations will become increasingly tenuous. Those who support retaining the status quo will be overtaken by events.

Some experts in favor of maintaining the current governance structure also argue that CISA[48] and DoD are highly capable SRMAs for the communications and DIB sectors, respectively. These experts argue that creating a space systems sector could (or would) undermine something that works well. Even the respondents who favor designating space systems as a new critical infrastructure sector emphasized that any new construct must avoid damaging elements of the current configuration that work well. Some experts supported a "carveout" within the space systems sector for communications and the DIB.

Even without thoroughly assessing the track record of DHS (CISA) and DoD as SRMAs, it is clear that there is room for improvement. A 2021 Government Accountability Office study, for example, warned that DHS has not updated the communications sector-specific plan since 2015. Thus, the "plan lacks information on new and emerging threats," including "disruptions to position, navigation, and timing services."[49] DoD, meanwhile, has not updated the DIB-specific plan since 2010.[50]

Proponents of the existing structure worry that designating space systems as a standalone sector could heighten the burdens borne by industry. The creation of a new sector inadvertently (or inevitably) could result in overlap and duplication of extant efforts, and new requirements — potentially regulatory in nature — could be introduced.

While these concerns are not without merit, the current regulatory environment is already untenable and unpredictable. According to a November 2022 study by MITRE and the Aspen Institute, operators seeking approvals for space missions "must adhere to several distinct regulatory policies and engage with several different government agencies on different technical aspects of their operation."[51] While the report stopped short of calling for the designation of space systems as a critical infrastructure sector, it urged the designation of "a single agency with responsibility and funding to authorize and oversee U.S. commercial missions." The report also warned that current regulatory policies put "the U.S. space industry at a competitive disadvantage."[52] A critical infrastructure sector designation would need to be accompanied by efforts to streamline and simplify regulatory compliance.

Finally, status quo advocates contend that if the requisite will and leadership existed, then just as much could be accomplished without a critical infrastructure designation as with one. The U.S. government could rapidly mobilize resources, including funding and information, to where they are needed for the security and resilience of space systems.

Even if this were so, the fact remains that no such action has occurred. The status quo cannot stand, particularly in an era when private companies conduct weekly or even daily launches of reusable systems and run their own space stations and commercial lunar operations. Either the United States leans forward and changes now, or it will be forced do so as a rearguard action when no other choice is available. By then, it may be too little, too late.

Having said that, there is also the understandable concern that adding to the number of designated critical infrastructure sectors will dilute focus on other priorities. The government's designation of the space systems sector as critical infrastructure may need to be accompanied by efforts to pare back the number of designated sectors (such as by combining certain existing sectors).[53]

Short of designating space systems as critical infrastructure, there is one other potential path forward: leveraging CISA's identification of national critical functions (NCFs). The NCF framework translates the functions of critical sectors into actions, such as "generate electricity" or "supply water," with the aim of addressing risk in a holistic way by better incorporating "cross-cutting risks and associated dependencies." At least within certain quarters of government, there is a distinct appetite for taking a functional (NCF) approach rather than issuing a new sector designation, because of a focus on cross-sector risk in the form of critical interdependencies.[54]

While cross-sector risk is undeniably important, the NCF approach has a significant shortcoming: There is not yet a natural way for government and industry to collaborate around functions. The NCF rubric focuses on "how entities come together to produce critical functions, and what assets, systems, networks, and technologies underpin those functions," and it is therefore

company-agnostic.[55] Critical infrastructure sector designations, by contrast, center on the companies that fall within a sector's ambit. Those companies, in turn, have forums to collaborate with one another and with the government to manage risks. This structure provides the foundation for the public-private partnership that is essential to safeguard space systems.

Whether for or against the designation of a new sector, interviewees broadly agreed that the federal government must better support the commercial space community by marshaling resources and sharing information related to threats, vulnerabilities, and incidents. Experts also repeatedly noted that government cybersecurity support and guidance, particularly for smaller companies lacking the wherewithal and expertise of larger firms, need improvements. Standards, if made more consistent across the board, could improve cybersecurity within the commercial space community while making compliance simpler and easier. Designating space systems as a critical infrastructure sector could provide a structure to help resolve all of these issues.

Defining the Sector and Its Public-Private Collaboration Mechanisms

Designating space systems as a critical infrastructure sector would likely result in a more coherent whole-of-government approach to strategy, policy, programs, and resources. It would also signal to actors inside and outside of government, as well as to allies and adversaries abroad, that space systems are a priority and will be treated accordingly. Sustaining focus over time will require concerted effort in terms of both leadership and resources.

Designating a sector requires defining its parameters. The term "space systems" captures the entire ecosystem from ground to orbit.[56] In addition, it includes sensors, signals, uplinks/downlinks and the data they transmit, payloads, applications, critical technologies, supply chains (including software, hardware, assembly, manufacturing, and servicing), and all of the people who support these components. This definition sets a minimum baseline. Parameters could and should be adjusted to encompass the further growth of space systems beyond geosynchronous orbit, into cislunar space, the lunar surface to the libration points, and the boundary of the gravitational influence of the Earth.

After defining the scope of the space sytems sector (in a flexible way that recognizes the rapidly changing technological and economic environment), the next question is: What agency should serve as SRMA? SRMAs take the lead on coordination within government and collaboration with private-sector partners to foster security and resilience. In some cases, an SRMA may have regulatory responsibilities. The role of the designated SRMA is multifaceted and, historically, has included leading or supporting:

- 1. sector risk management, such as through programs to help mitigate threats and vulnerabilities;
- 2. sector (as well as national) risk assessment efforts;
- 3. sector coordination, such as by "participating in cross-sector coordinating councils";
- 4. information sharing related to physical security and cybersecurity threats, in real time when possible;
- 5. incident management, such as through "restoration efforts"; and
- 6. emergency preparedness, such as through exercises.[57]

When asked which agency they see as best positioned to become the SRMA, expert opinions varied widely.[58] Overall, DHS (CISA) and DoD's Space Force were most frequently proposed for the SRMA role — but not without caveats.

Experts view CISA as well suited to engage with the private sector, but were concerned that the agency is already spread too thin. CISA also lacks any space-specific capacity, although it has begun to give the space sector more vigorous attention. Respondents, meanwhile, had confidence in DoD's core capabilities but questioned whether DoD was best placed to engage with the commercial sector. Designating DoD as SRMA would also likely crowd out other crucial actors. Significantly, DoD is also relatively weak on economic analysis. Regarding the Space Force in particular, several experts underscored that it already had a full plate.

The Department of Commerce, the Department of Transportation, and NASA were mentioned next-most often as proposed SRMA. Experts warned, however, that Commerce and Transportation have yet to mature their protective capabilities, while experts argued that NASA should be left to pursue its important and robust non-security mission.

Given the limitations of each of the proposed agencies, the authors also asked experts whether more than one entity should be charged with leading the sector. Three existing critical infrastructure sectors are co-led: food and agriculture, government facilities, and transportation systems.[59] Here, too, opinion was divided. Some experts favored the idea of co-SRMAs because of the multiplicity of equities involved.[60] Others rejected it as unworkable over time, noting that "partnership works until it does not." As a practical matter, the authors believe that a single overall lead would best serve U.S. interests — but this would require meaningful consultation and collaboration with partners inside and outside government.

Despite concerns expressed by some interviewees, the authors see NASA as best placed to serve as lead SRMA for the space systems sector, given its sector-specific capability (which the experts repeatedly lauded) and its proven ability to partner effectively with the private sector. NASA has an extraordinary record of innovation and achievement, which resonates with industry, from the largest companies to smaller businesses. This offers a platform upon which to build a close and constructive working relationship with the private sector, so long as NASA deftly handles the possibility that some in the private sector may view the agency in part as a competitor. NASA also understands both the economics and the diplomacy of space.

Asking NASA to undertake this task, however, will require it to commit to the mission, and NASA has yet to demonstrate interest in becoming an SRMA. Investment is equally imperative: As outlined in the recommendations section, NASA must be given the extra resources necessary to fulfill its new responsibilities, and relevant congressional committees must commit to the mission. Serving as SRMA must not compromise NASA's other important work. To be clear, the SRMA role would require NASA to develop and scale up its capacity to protect national security, civil, and commercial space systems, which support national and economic security and other critical infrastructure.

Maintaining subgroups within the sector to preserve the autonomy and effectiveness of the communications and DIB components would further refine what is being asked of NASA. Notably, specific segments of the energy sector (electricity, and oil and gas) are also addressed by subgroups tailored to segment needs and priorities. Within the space systems sector, DoD could continue to serve as the SRMA for defense and intelligence systems, while the FCC would continue to regulate space-based communications systems. By the nature of its position within the White House, meanwhile, the National Space Council (chaired by the vice president), has unique abilities to ensure interagency cooperation among these agencies and between NASA and other federal partners.

Two other elements of sector governance that are required for effective critical infrastructure security are the sector coordinating council (SCC) and government coordinating council (GCC). SCCs are "self-organized and self-governed" nongovernmental groups that bring together "critical infrastructure owners and operators, their trade associations, and other industry representatives." Industry associations, which have members and are collaborating already, are well equipped to play a constructive role in building SCCs, which act as "the sector's voice" and "facilitate the government's collaboration with the sector for critical infrastructure security and resilience activities."[61] SCCs may pursue a range of functions, such as identifying and disseminating (sector-applicable) best practices for cybersecurity.

SCC members designate their representatives, who may be senior executives but typically are not CEOs. In the energy sector, however, the charter of the Electricity Sub-Sector Coordinating Council (ESCC) specifies that the ESCC "consists of CEO level representatives."[62] By virtue of this feature, the ESCC can quickly mobilize resources and execute decisions. This particular element is worthy of emulation: A CEO-level SCC would benefit the space systems sector.

GCCs, meanwhile, take the lead on coordinating "strategies, activities, policy, and communications across governmental entities within each sector."[63] The GCC is distinct from the SRMA but is chaired by an SRMA representative.[64] In the case of space systems, the GCC would involve the range of departments and agencies referenced above with equities in space systems' security. GCCs could also include state and local governments as needed. Experts interviewed for this report noted that the strongest model is one in which the SCC and GCC work together effectively. Here again, the energy sector was cited as exemplary.

Finally, to develop information sharing throughout the sector, NASA can rely on existing ISAC initiatives. The Space ISAC's watch center, for example, is expected to achieve initial operating capability this year.

Recommendations

Space systems are critical to U.S. national and economic security and are destined to become increasingly so. The status quo falls short of reflecting and adapting to this reality. Despite pockets of excellence, there are too many gaps in the current U.S. posture that give rise to unacceptable vulnerabilities — especially when the space domain grows ever more "congested, contested, and competitive."[65] A more concerted and coherent approach is needed. Designating space systems as a critical infrastructure sector would serve that end, signaling inside and outside the country that space security and resilience is a top priority and thereby jump-starting a whole-of-nation effort.

In offering these recommendations, the authors are mindful that the Biden administration is conducting a larger review of the nation's critical infrastructure framework and policy. In concert with that effort, this paper proposes the following:

For the Executive Branch

Recommendation 1: Designate space systems as a critical infrastructure sector, wherein the entire ecosystem from ground to orbit is included in the definition of space systems. The sector should quickly set to work formulating a sector-specific plan that includes a sectoral definition and priorities.

1.1 – Designate NASA as the SRMA for the space systems sector. Managing risk in this sector requires expertise in national security, economic analysis, and science and technology, among other things. NASA has the necessary expertise and thus should be the overall lead. The agency, however, should not be tasked with an unfunded mandate. (See Recommendation 2.) NASA must be resourced to develop and scale up its capacity to be an SRMA. As outlined in subsequent recommendations, it is also imperative that commercial entities be deeply integrated into the governance of the space systems sector.

1.2 – Create two directed subgroups within the sector, one for DoD and the intelligence community and another for communications. DoD would continue to lead within its own sphere of responsibility, just as it does now, and the Space Force would serve as the department's executive agent. With regard to communications, the subgroup should be subservient to the larger communications sector, which is already designated as critical infrastructure, with the FCC maintaining its current regulatory role. The subgroups are intended to avert disruption while reconfiguring U.S. posture. Here the authors are mindful of the adage, "If it ain't broke, don't fix it."

1.3 – Do not assign the SRMA a regulatory role. Space systems are already regulated through other rule sets. Mechanisms for mission authorization and other certifications should support timely decision-making, without undue lags that unnecessarily inhibit operators or stifle innovation. Compliance with existing regulations should be streamlined and simplified, but creating a regulatory role for NASA will not help in that regard.

1.4 – Articulate and offer industry a clear value proposition. The federal government should specify the benefits of designating a new sector and demonstrate in both word and deed that industry will not be subject to additional burdens due to overlaps with already-existing critical infrastructure sectors or duplication of their requirements. Even the strongest case will not make itself. The federal government must conduct concerted outreach to the commercial sector, including smaller companies that are highly innovative but relatively new entrants to the market. The added value of creating a new sector inheres in coordinating strategy, policy, resources, and programs to support the designated infrastructure — in tandem with an enhanced version of public-private partnership. For example, industry has repeatedly expressed a desire for government to share information at scale but in a tailored way that relays high-priority information rather than causing overload. The federal government should deliver on this request, establishing a whole-of-government architecture that also supports two-way flow between the public and private sectors and ultimately integrates key foreign partners in the space systems sector. In addition, the federal government should provide guidance and support, such as programs and resources, to elevate levels of resilience

and cybersecurity on the commercial side — including in supply chains, where smaller companies may feature prominently but lack the wherewithal or awareness to properly protect themselves and all those they serve.

1.5 – Strengthen international norms and standards. In addition to sector designation, which provides an opportunity to enhance U.S. collaboration with global partners on critical infrastructure policy, the federal government needs a multipronged strategy to address the international dimension of threats to, and opportunities for, space systems. The strategy should communicate to U.S. allies, competitors, and adversaries how important space is to the United States — and that there will be significant consequences for threatening or compromising U.S. space systems. Washington will need to lead by example and work with allies and industry to establish and strengthen internationally accepted norms of responsible behavior in space.[66] Matters for future study include whether to revisit and rewrite the Outer Space Treaty, whether a "Five Eyes Plus" space council is needed, and whether to build on the foundation of the Artemis Accords — and if so, how. The U.S. government should also work with partners and allies to harmonize standards in recognition of the fact that not all of the infrastructure in this sector is U.S.-based, U.S.-built, or U.S.-operated. In pursuing this work, the challenge is to coordinate domestic governance measures with companion efforts at the international level so as to minimize disjunctures between the two.

1.6 – Integrate the National Space Council into the governance of the space systems sector. Well-thought-out policy and strategy are integral to coherent and effective operations. The work of the Space Council on priority-setting and other high-level matters should be tightly tied to, and aligned with, the operational arms of the sector in order to achieve successful implementation and optimize resource allocation. Successful integration of the National Space Council will assist NASA as the SRMA by enabling smooth interagency collaboration.

For Congress

Recommendation 2: Give NASA, the lead SRMA, the resources to effectively accomplish the mission. Congress should allocate, authorize, and appropriate supplemental funding — an initial investment of $15 million per year — to NASA to allow it to successfully take on the responsibilities of lead SRMA for the space systems sector. Over time, this number may grow. Too often, SRMAs have been assigned a mandate without any corresponding new funding. In this respect, the energy sector is an exception to the general rule. Policy without resources is merely rhetoric. Forcing NASA, whether by design or effect, to fulfill the role of SRMA at the expense of other important ongoing work would not serve the country well.

This new funding would support a full operating capability of 25 fulltime employees with responsibilities related to stakeholder engagement, programs, exercises, and other activities needed to protect national security, civil, and commercial systems, which in turn support national and economic security and other critical infrastructure. Under this vision, the sector's operations center would be outsourced to a third party and could build upon existing initiatives in this area.

2.1 – Direct the Congressional Research Service to undertake a legislative review to determine what legislation is needed to account for the expansion of commercial space operations. Existing legislation may be out of date. The proposed study would identify current gaps, shortfalls, and shortcomings.

For Industry

Recommendation 3: Marshal and organize the commercial space community to play an instrumental role in governance of the space systems sector in order to enhance the security and resilience of this critical infrastructure.

3.1 – Establish a space systems sector coordinating council that by charter must consist of CEO-level representatives. This will ensure that decisions are backed up by resource allocation to support implementation. The chair of the space systems SCC should be the CEO of a U.S. company.

3.2 – Task the space systems SCC, through its charter, with working to reduce risks to the security and resilience of the commercial space sector. These efforts should include conducting annual assessments, monitoring systems to provide sectoral awareness, communicating vulnerabilities and lessons learned, and helping industry constituents reach their highest security potential in terms of planning and operations. The idea here is to empower and encourage those with the deepest knowledge of industry operations to work to identify, assess, and manage risks. The space systems SCC, in striving to accomplish

its mission, must deal effectively with the full spectrum of needs of the many and varied companies in the sector. This includes the newer and smaller entities, which may be bringing to market unprecedented innovations and occupy an important place in supply chains yet lack the bandwidth or expertise to recognize and remedy significant cyber and other vulnerabilities.

3.3 – Leverage and build upon the existing work of ISACs (including the Space ISAC) to establish a watch center capability and a cyber vulnerability lab, among other things. These efforts are being pursued together with partners worldwide and should be expanded and leveraged wherever possible.

For Industry and Government Together

Recommendation 4: Create a co-led risk management enterprise. The pivotal place of industry within the space systems sector requires an enhanced model of public-private partnership under which the risk management enterprise is genuinely co-led.

4.1 – Jointly elaborate and widely implement cybersecurity best practices, including practices that specifically address the challenges inherent in, and unique to, the space systems sector.[67] This effort should encompass both information technology and operational technology. Federal systems follow guidance from the National Institute of Standards and Technology, whose cybersecurity resources for commercial space systems are also relevant.[68] Guidance for space systems should also include the guidance of the International Organization for Standardization. Industry should voluntarily adhere to the principles of security by design and the framework of cyber-informed engineering. It should also strive to optimize supply chain resources by working to minimize the injection or importation of problematic services, technologies, and intellectual property. To the extent possible, government procurement should reinforce advocacy of best practices.

4.2 – Pair commercial and government capabilities to model a dynamic risk environment that could anticipate threat and adversary tactics, techniques, and procedures. This effort should include extensive war-gaming and tabletop exercises to discover what technologies could be disruptive and to help decide how best to prepare for them.

4.3 – Add space assets positioned outside of traditional operational areas to enhance U.S. resilience. Diversification is a prudent strategy here, just as in many other contexts.

Conclusion

Space systems are inextricably and increasingly intertwined with the national and economic security of the United States. Few dispute the criticality of these systems, but there is significant variance of opinion on how best to protect them. The coming era of ubiquitous human and robotic space systems will decisively shift all narratives pertaining to the status quo. After soliciting a range of views and exploring a range of possibilities, one way forward stands out: designating space systems as a critical infrastructure sector. From a practical standpoint, it may be difficult to obtain the agreement necessary among key decision-makers and stakeholders for defining and designating a new sector. This challenge should not be underestimated, but it is not insurmountable if the case is made strongly, the imperative is clear, and a workable action plan is offered. No other option holds greater potential for enhancing U.S. resilience and cybersecurity and kick-starting a whole-of-nation effort to support and advance continued U.S. leadership in the space domain — and the multitude of endeavors dependent upon it.

Appendix: Selected List of Subject Matter Experts Interviewed

This list does not imply that the experts or any organizations with which they are affiliated endorse the recommendations in this paper.

Pat Arvidson
Former Technical Director and Former Principal Cyber Advisor for the Secretary of Defense, Department of Defense

Michael Bloxton
Chairman and CEO, Nebula Compute, Inc.

Kerry Buckley
Vice President & FFRDC Director, Center for Advanced Aviation System Development, MITRE

Kathryn Condello
Senior Director, National Security/ Emergency Preparedness, Lumen Technologies; Vice Chair, Communications Sector Coordinating Council

Lori Gordon
Systems Director for the Office of the Corporate Chief Engineer, The Aerospace Corporation

Susan M. Gordon
Former Principal Deputy Director of National Intelligence; Former Deputy Director of the National Geospatial Agency

Brian Harrell
Former Assistant Secretary for Infrastructure Protection, Department of Homeland Security

Bob Kolasky
Senior Vice President, Exiger; Former Director of the National Risk Management Center, Department of Homeland Security

Lt. Gen. Steven L. Kwast, USAF, Ret.
CEO, Skycorp Inc.

Katherine Ledesma
Senior Director, Government Affairs, Dragos, Inc.

Charles Miller
Co-founder and CEO, Lynk; Former Senior Advisor for Commercial Space, NASA

Erin Miller
Executive Director, Space Information Sharing and Analysis Center

David Mussington
Executive Assistant Director for Infrastructure Security, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security

Jonathan Neal
Executive Director, Space Policy, U.S. Chamber of Commerce

Maj. Gen. John M. Olson
Mobilization Assistant to the Chief of Space Operations and Space Force Lead for JADC2 and ABMS, United States Space Force; Chief Data and AI Officer, Department of the Air Force

Scott Pace
Director, Space Policy Institute, The George Washington University; Former Deputy Assistant to the President and Executive Secretary, National Space Council

Steve Pann
Co-founder and Managing Partner, Razor's Edge Ventures

Jonathan Pettus
Senior Vice President of Aerospace, Defense, and Civil Operations, The Dynetics Group

Lt. Gen. Harry D. Raduege, Jr., USAF, Ret.
Chief Executive Officer, The National Cybersecurity Center; Senior Counselor, The Cohen Group

Nicholas Reese
Deputy Director for Emerging Technology Policy, Department of Homeland Security

Christopher Roberti
Senior Vice President for Cyber, Space, and National Security Policy, U.S. Chamber of Commerce

Walter Scott
Executive Vice President and Chief Technology Officer, Maxar Technologies

Steve Shirley
Executive Director, The National Defense Information Sharing and Analysis Center

Samuel Visner
Former Director, National Cybersecurity FFRDC, MITRE ; Tech Fellow, The Aerospace Corporation: Vice Chair, Space Information Sharing and Analysis Center

Vincent Voci
Vice President for Cyber Policy and Operations, U.S. Chamber of Commerce

Jennifer Warren
Vice President of Civil and Regulatory Affairs, Lockheed Martin

Bradley Whittington
Vice President of Engineering, The Dynetics Group

Christy K. Wilder
Vice President and Chief Security Officer, Maxar Technologies

Renee Wynn
Former Chief Information Officer, NASA

David Zikusoka
Special Assistant to the Secretary of Defense, U.S. Department of Defense

Endnotes

1. Bryan Bender, "'We better watch out': NASA boss sounds alarm on Chinese moon ambitions," *Politico*, January 1, 2023. (https://www.politico.com/news/2023/01/01/we-better-watch-out-nasa-boss-sounds-alarm-on-chinese-moon-ambitions-00075803)

2. "Space Foundation Releases the Space Report 2022 Q2 Showing Growth of Global Space Economy," *Space Foundation*, July 27, 2022. (https://www.spacefoundation.org/2022/07/27/the-space-report-2022-q2)

3. U.S. Office of the Director of National Intelligence and Department of Defense. "National Security Space Strategy: Unclassified Strategy," January 2011. (https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2011_nationalsecurityspacestrategy.pdf)

4. The White House, "Presidential Policy Directive -- Critical Infrastructure Security and Resilience," February 12, 2013. (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)

5. Historically, however, the phrase "space systems" may have been understood more narrowly.

6. Some contend that space is a domain and only a domain, as opposed to an infrastructure. As a domain, space is like cyber in that both transcend all other domains.

7. The White House, "Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems," September 2020. (https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems)

8. Edward Swallow and Samuel Visner, "Opinion: It's Time to Declare Space Systems as Critical Infrastructure," *Politico*, April 2, 2021. (https://www.politico.com/news/2021/04/02/its-time-to-declare-space-systems-as-critical-infrastructure-478848)

9. Interview with subject matter experts.

10. Interview with a subject matter expert.

11. Interview with subject matter experts. Others estimate that it will take until 2040 to reach or surpass the $1 trillion mark. See, for example: Michael Sheetz, "The Space Industry Is on Its Way to Reach $1 Trillion in Revenue by 2040, Citi Says," *CNBC*, May 21, 2022. (https://www.cnbc.com/2022/05/21/space-industry-is-on-its-way-to-1-trillion-in-revenue-by-2040-citi.html); "Space: Investing in the Final Frontier," *Morgan Stanley Research*, July 24, 2020. (https://www.morganstanley.com/ideas/investing-in-space)

12. Tina Highfill, Annabel Jouard, and Connor Frank, U.S. Bureau of Economic Analysis, "Updated and Revised Estimates of the U.S. Space Economy, 2012–2019," January 2022. (https://www.bea.gov/data/special-topics/space-economy). Note that the 2021 figure is more than five times the revenue generated in the railway sector for the same period and is twice the projected income of the airline sector for 2021. "Rail Transportation Industry in the US - Market Research Report," *IBISWorld*, January 2023. (https://www.ibisworld.com/united-states/market-research-reports/rail-transportation-industry); "Economic Performance of the Airline Industry," *IATA*, October 2021. (https://www.iata.org/en/iata-repository/publications/economic-reports/airline-industry-economic-performance---october-2021---report)

13. U.S. National Aeronautics and Space Administration, "Economic Impact Report," October 2022. (https://www.nasa.gov/sites/default/files/atoms/files/nasa_fy21_economic_impact_report_brochure.pdf)

14. SpaceX alone has launched more advanced-technology spacecraft in its Starlink constellation than the Department of Defense has launched in the last 50 years — and this is only poised to accelerate in coming years. Interview with a subject matter expert.

15. Laura Grego, "A History of Anti-Satellite Programs," *Union of Concerned Scientists*, January 2012. (https://www.ucsusa.org/sites/default/files/2019-09/a-history-of-ASAT-programs_lo-res.pdf)

16. Secretary of State Antony Blinken, U.S. Department of State, Press Statement, "Russia Conducts Destructive Anti-Satellite Missile Test," November 2021. (https://www.state.gov/russia-conducts-destructive-anti-satellite-missile-test)

17. UK Foreign, Commonwealth, and Development Office, Press Release, "Russia behind Cyber-Attack with Europe-Wide Impact an Hour before Ukraine Invasion," May 2022. (https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion)

18. Valerie Insinna, "SpaceX Beating Russian Jamming Attack Was 'Eyewatering': DOD Official." *Breaking Defense*, April 2022. (https://breakingdefense.com/2022/04/spacex-beating-russian-jamming-attack-was-eyewatering-dod-official)

19. Sandra Erwin, "Russia Escalates Rhetoric on Commercial Satellites, Calls Them 'Legitimate Targets for Retaliation,'" *Space News*, October 2022. (https://spacenews.com/russia-escalates-rhetoric-on-commercial-satellites-calls-them-legitimate-targets-for-retaliation)

20. Christian Vasquez, "CISA Researchers: Russia's Fancy Bear Infiltrated US Satellite Network," *CyberScoop*, December 16, 2022. (https://www.cyberscoop.com/apt28-fancy-bear-satellite)

21. U.S. Government Accountability Office, "National Security Snapshot: Challenges Facing DOD in Strategic Competition with China," February 2022. (https://www.gao.gov/products/gao-22-105448)

22. U.S. Department of Defense, "Military and Security Developments Involving the People's Republic of China," November 2022, page 68. (https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/1/2022-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF)

23. Ibid., page 89.

24. Ibid., page 72.

25. Input from a subject matter expert.

26. Chuck Brooks, "The Urgency to Cyber-Secure Space Assets," *Forbes*, February 27, 2022. (https://www.forbes.com/sites/chuckbrooks/2022/02/27/the-urgency-to-cyber-secure-space-assets); Brandon Bailey, "Cybersecurity Protections for Spacecraft: A Threat Based Approach," *The Aerospace Corporation*, July 15, 2022. (https://aerospace.org/research/cybersecurity-protections-spacecraft-threat-based-approach); "Space Attack Research & Tactic Analysis," *The Aerospace Corporation*, accessed March 14, 2023. (https://sparta.aerospace.org)

27. Tereza Pultarova, "Russian space debris forces space station to dodge, delays US spacewalk," *Space.com*, December 21, 2022. (https://www.space.com/russian-space-debris-cancels-nasa-spacewalk); Tariq Malik, "International Space Station dodges orbital debris from Russian anti-satellite test," *Space.com*, June 19, 2022. (https://www.space.com/space-station-dodges-russian-satellite-debris)

28. The United States has launched both public and private sector space assets from coastal sites abroad. The White House, "United States Space Priorities Framework," December 2021. (https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Space-Priorities-Framework-_-December-1-2021.pdf)

29. U.S. Department of Homeland Security, Cybersecurity and Infratructure Security Agency, Press Release, "CISA Launches a Space Systems Critical Infrastructure Working Group," May 13, 2021. (https://www.cisa.gov/news/2021/05/13/cisa-launches-space-systems-critical-infrastructure-working-group)

30. U.S. Department of Homeland Security, Cybersecurity and Infratructure Security Agency, "FY 2021 National Defense Authorization Act: Section 9002(b) Report," November 12, 2021. (https://www.cisa.gov/sites/default/files/publications/Section_9002_NDAA_Report_FINAL_508c.pdf)

31. The White House, "Letter from the President to Select Congressional Leadership on the Nation's Critical Infrastructure," November 7, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/07/letter-from-the-president-to-select-congressional-leadership-on-the-nations-critical-infrastructure)

32. U.S. Department of Homeland Security, Cybersecurity and Infratructure Security Agency, "FY 2021 National Defense Authorization Act: Section 9002(b) Report," November 12, 2021, pages 44 and 49-50. (https://www.cisa.gov/sites/default/files/publications/Section_9002_NDAA_Report_FINAL_508c.pdf)

33. Ibid., page 2.

34. The White House, "National Cybersecurity Strategy," March 2023, page 6. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)

35. The White House, "National Space Council," accessed March 14, 2023. (https://www.whitehouse.gov/spacecouncil)

36. Theresa Hitchens, "Industry squabbles on need for novel space regulation as White House deliberates," *Breaking Defense*, March 17, 2023. (https://breakingdefense.com/2023/03/industry-squabbles-on-need-for-novel-space-regulation-as-white-house-deliberates)

37. The White House, "Readout of Space Systems Cybersecurity Forum Hosted by the Office of the National Cyber Director and the National Space Council," March 28, 2023. (https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/28/readout-of-space-systems-cybersecurity-executive-forum-hosted-by-the-office-of-the-national-cyber-director-and-the-national-space-council/)

38. Satellite Cybersecurity Act, S.3511, 117th Congress (2022). (https://www.congress.gov/bill/117th-congress/senate-bill/3511)

39. U.S. Senate Committee on Homeland Security and Governmental Affairs, Press Release, "Peters, Cornyn Introduce Bipartisan Legislation to Protect Commercial Satellites from Cybersecurity Threats," January 19, 2022. (https://www.hsgac.senate.gov/media/majority-media/peters-cornyn-introduce-bipartisan-legislation-to-protect-commercial-satellites-from-cybersecurity-threats). Separately, in January 2023, the National Institute of Standards and Technology issued new guidance on how to apply its cybersecurity framework to satellite ground segment operations. Suzanne Lightman, Theresa Suloway, and Joseph Brule, U.S. National Institute of Standards and Technology, "Applying the Cybersecurity Framework to Satellite Command and Control: NIST Interagency Report (IR) 8401," January 3, 2023. (https://www.nist.gov/news-events/news/2023/01/applying-cybersecurity-framework-satellite-command-and-control-nist)

40. Space Infrastructure Act, H.R.3713, 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/house-bill/3713/text)

41. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4050. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

42. Interview with subject matter experts.

43. The authors asked each interviewee the same questions, with adjustments made only as needed on a case-by-case basis. Regardless of whether or not the interlocutors favored creating a standalone sector, the authors sought their thoughts on how to structure such a sector.

44. Interviews with subject matter experts.

45. U.S. Department of Homeland Security, Cyber and Infrastructure Security Agency, "Communications Sector-Specific Plan An Annex to the NIPP 2013," 2015. (https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf)

46. It can be argued, however, that once in operation, these systems are the property of DoD, as the DIB covers their production, not their operation.

47. Edward Swallow and Samuel Visner, "Space Is Critical Infrastructure; Securing It Is a National Imperative," *Space ISAC*, July 29, 2021. (https://s-isac.org/space-is-critical-infrastructure-securing-it-is-a-national-imperative)

48. PPD-21 designates DHS rather than CISA as the SRMA, but DHS delegated that responsibility to CISA.

49. U.S. Government Accountability Office, "Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector," November 2021. (https://www.gao.gov/assets/gao-22-104462.pdf)

50. U.S. Department of Homeland Security, Cyber and Infrastructure Security Agency, and Department of Defense, "Defense Industrial Base Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan," May 2010. (https://www.cisa.gov/publication/nipp-ssp-defense-industrial-base-2010)

51. "The Space Imperative: A Whole-of-Nation Approach to a Sustainable, Secure, and Resilient Space Domain," *MITRE Corporation* and *Aspen Institute*, November 2022, page 2. (https://www.mitre.org/sites/default/files/2022-11/pr-22-3156-space-imperative-whole-of-nation-approach-sustainable-secure-resilient-space-domain.pdf)

52. Ibid., page 7.

53. Interview with a subject matter expert.

54. Ibid.

55. U.S. Department of Homeland Security, Cybersecurity and Infratructure Security Agency, "National Critical Functions," accessed March 14, 2023. (https://www.cisa.gov/national-critical-functions)

56. Historically, however, the phrase "space systems" may have been understood more narrowly.

57. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4768. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

58. Experts offered a multitude of suggestions: the Department of Commerce, the Department of Defense (Space Force/Space Command), the Department of Homeland Security (CISA), the Department of State, the Department of Transportation (FAA), the National Aeronautics and Space Administration (NASA), and the FCC. The Department of the Treasury and the Intelligence Community were also deemed to have a stake in the sector but were not proposed for a lead role in sector risk management. The National Space Council was mentioned as well but was deemed to be too strategic and insufficiently operational by design.

59. They are led by the Department of Agriculture and the Department of Health and Human Services, by DHS and the General Services Administration, and by DHS and the Department of Transportation, respectively.

60. Some of the experts in favor of co-SRMAs took the idea a step further, raising the possibility of rotating SRMAs — and even the possibility of a commercial entity as co-leader. However, current law requires the SRMA to be a federal department or agency.

61. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Sector Coordinating Councils," accessed March 14, 2023. (https://www.cisa.gov/resources-tools/groups/sector-coordinating-councils)

62. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Electricity Sub-Sector Coordinating Council Charter," August 5, 2013, page 3. (https://www.cisa.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf)

63. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Government Coordinating Councils," accessed March 14, 2023. (https://www.cisa.gov/resources-tools/groups/government-coordinating-councils)

64. A senior CISA official generally co-chairs all GCCs. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Government Coordinating Councils," accessed March 14, 2023. (https://www.cisa.gov/resources-tools/groups/government-coordinating-councils)

65. U.S. Office of the Director of National Intelligence and U.S. Department of Defense, "National Security Space Strategy: Unclassified Strategy," January 2011. (https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2011_nationalsecurityspacestrategy.pdf)

66. For example, the White House announced in April 2022 that the United States "commits not to conduct destructive, direct-ascent anti-satellite (ASAT) missile testing, and … seeks to establish this as a new international norm for responsible behavior in space." The White House, "Fact Sheet: Vice President Harris Advances National Security Norms in Space," April 19, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/18/fact-sheet-vice-president-harris-advances-national-security-norms-in-space/)

67. These practices include cross-sector cybersecurity performance goals and cyber hygiene recommendations that apply across the board to critical infrastructure. U.S. Department of Homeland Security, Cyber and Infrastructure Security Agency, "Cross-Sector Cybersecurity Performance Goals," Cybersecurity and Infrastructure Security Agency, accessed March 14, 2023. (https://www.cisa.gov/cross-sector-cybersecurity-performance-goals)

68. Matthew Scholl, "Exploring Cyber Space: Cybersecurity Issues for Civil and Commercial Space Systems," *Testimony Before the House Committee on Science, Space and Technology Subcommittee on Space and Aeronautics*, July 28, 2022. (https://www.nist.gov/speech-testimony/exploring-cyber-space-cybersecurity-issues-civil-and-commercial-space-systems); Suzanne Lightman, Theresa Suloway, and Joseph Brule, U.S. National Institute of Standards and Technology, "Applying the Cybersecurity Framework to Satellite Command and Control: NIST Interagency Report (IR) 8401," January 3, 2023. (https://www.nist.gov/news-events/news/2023/01/applying-cybersecurity-framework-satellite-command-and-control-nist)

About the Authors

Frank Cilluffo is the director of the McCrary Institute for Cyber and Critical Infrastructure Security at Auburn University. He was a member of the Cyberspace Solarium Commission and is a distinguished advisor to CSC 2.0. Frank previously served on the Department of Homeland Security's Advisory Council, chairing the economic security subcommittee. Following the attacks on September 11, 2001, Frank served as a special assistant to President George W. Bush for homeland security and as a principal advisor to U.S. Secretary of Homeland Security Tom Ridge.

RADM (Ret.) Mark Montgomery is the senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies. He also directs CSC 2.0, having served as the Cyberspace Solarium Commission's executive director. Previously, Mark served as policy director for the Senate Armed Services Committee, coordinating policy efforts on national security strategy, capabilities and requirements, and cyber policy. Mark served for 32 years in the U.S. Navy as a nuclear-trained surface warfare officer, retiring as a rear admiral in 2017.

Sharon Cardash is deputy director for policy at Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security. Before joining Auburn, she served as deputy director of The George Washington University's Center for Cyber and Homeland Security. She holds degrees in law and international relations, and her writings have appeared in policy publications, scholarly journals, and major newspapers.

Kelsey Shields is a research analyst for policy at Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security. She holds degrees in political science and international relations, with thematic focuses in international security policy and nuclear studies and a regional focus in Asia. Her work has been published in major newspapers.

ACKNOWLEDGEMENTS

The following individuals kindly served as peer reviewers of an earlier draft of this paper, and we are most grateful for the insights and time they contributed: Michael Klipstein, Robert Kolasky, Steven Kwast, Katherine Ledesma, Bruce Pittman, Samuel Visner, and Dennis Wingo. Their acknowledgment here does not imply their endorsement of the recommendations in this paper. We are also grateful to Annie Fixler, Daniel Ackerman, David Adesnik, Erin Blumenthal, John Hardie, Miriam Himmelfarb, and David May for their work on the production of this report.

Cover Photo: A Lockheed Martin Atlas 5 rocket lifts off at the Kennedy Space Center in Cape Canaveral, Florida. (Photo by Matt Stroshane/Getty Images).

The views of the authors do not necessarily reflect the views of CSC 2.0's distinguished advisors, senior advisors, or any affiliated organizations or individuals.

About CSC 2.0

CSC 2.0 is preserving the legacy and continuing the work of the Cyberspace Solarium Commission (CSC). Congress created the CSC in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The commission operated successfully for two and a half years, publishing its flagship report in March 2020 along with subsequent white papers. The CSC issued more than 80 recommendations to reform U.S. government structures and organization, strengthen norms and non-military tools, promote national resilience, reshape the cyber ecosystem, operationalize public-private collaboration, and preserve and employ military instruments of national power.

At the CSC's planned sunset, the commissioners launched the CSC 2.0 project to support continued efforts to implement outstanding CSC recommendations, provide annual assessments of the implementation of CSC recommendations, and conduct research and analysis on several outstanding cybersecurity issues identified during the commission's tenure.

For more information, visit **www.CyberSolarium.org**.

Co-Chairmen

Angus S. King Jr., U.S. Senator for Maine

Michael "Mike" J. Gallagher, U.S. Representative for Wisconsin's 8th District

Distinguished Advisors

Frank J. Cilluffo, Director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security

Thomas A. "Tom" Fanning, Chairman, President, and Chief Executive Officer of Southern Company

James R. "Jim" Langevin, Former U.S. Representative for Rhode Island's 2nd District

Patrick J. Murphy, Former Acting Secretary and Under Secretary of the U.S. Army & Former U.S. Representative for Pennsylvania's 8th District

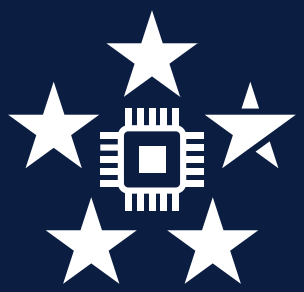
Samantha F. Ravich, Chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Benjamin E. "Ben" Sasse, Former U.S. Senator for Nebraska

Suzanne E. Spaulding, Senior Adviser for Homeland Security at the Center for Strategic and International Studies

Partners

FDD | McCRARY INSTITUTE FOR CYBER AND CRITICAL INFRASTRUCTURE SECURITY



CSC 2.0

Preserving and Continuing the Cyberspace Solarium Commission