INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

NOVEMBER 2021

Designating the U.S. Space Sector as Critical Infrastructure

Presented by

INSA'S CYBER COUNCIL

Building a Stronger Intelligence Community

EXECUTIVE SUMMARY

It is in the national interest to designate space systems as a sector of the critical infrastructure of the United States. As commercial companies have driven significant technological innovation and growth in the space sector, space-related technologies and systems have become increasingly critical to U.S. national and economic security. Designation of space as a critical infrastructure sector would enable public-private collaboration and information-sharing regarding both the space sector's vulnerabilities and the threats space assets face.

Designation would also clarify government agencies' roles and responsibilities in protecting space infrastructure, make clear to U.S. adversaries that the United States is committed to defending its space infrastructure, contribute to the establishment of global norms regarding the safety and security of space systems, and accelerate development of best practices and technologies for ensuring space security and resilience.

BACKGROUND

The space systems sector includes mission control, launch facilities, and an increasingly diverse supply chain. It consists today of more than 3,300 satellites, with tens of thousands of new satellites planned and around 1,300 being launched each year. Moreover, the sector encompasses hybrid architectures that include both older space system assets and systems using the latest technology.[1]

The expansion of commercial companies into the full range of space-based activities – including payload design and production, satellite launch, space-based internet, and human spaceflight – has driven unprecedented growth in the space sector in recent years. Some experts predict the value of the space industry will reach almost $1.5 trillion by the end of 2030.[2] Both civilian and government entities are becoming increasingly reliant on space-based and supporting infrastructure for the provision of key services such as position, navigation, and timing (PNT). Many of the National Critical Functions[3] noted by the U.S. Department of Homeland Security depend on space systems. The senior Department of Defense (DoD) official responsible for space policy characterized space-based capabilities in May 2021 as "critical to our modern economy, our democratic society, our way of life, and, yes, our military power."[4]

In September 2020, the White House National Space Council issued its Space Policy Directive-5 (SPD-5), which provides basic guidance on cybersecurity principles for space systems.[5] Since then, multiple industry and civic organizations have advocated for the designation of the U.S. space sector as critical infrastructure.[6] Due to its greater share of – and reliance on – space assets,[7] the United States is uniquely vulnerable compared to other countries – particularly as U.S. adversaries develop increasingly effective anti-satellite capabilities.

POLICY CONTEXT

SPD-5 elevated cyber threats to space systems as a key issue of national importance. However, existing space cybersecurity frameworks only partially address key aspects of space infrastructure. For example, precision navigation and timing (PNT) and space traffic management (STM) are covered under an existing National Institute for Standards and Technology framework and a White House Space Policy Directive, respectively, but important support infrastructure – including satellite control ground stations not related to national security – remain outside these guidelines.[8] Further, SPD-5 provides guidance, but no enforcement mechanisms, to maintain the security of space assets. Given the substantial costs of bringing existing space systems into compliance with cybersecurity standards, financial incentives and other benefits would encourage companies to adopt standards in a more timely, robust way.

The lack of comprehensive guidance, accountability mechanisms, and appropriate incentives to drive the adoption of cybersecurity standards to protect space assets places the space sector at significant risk, whether from U.S. adversaries or unanticipated crises. Given the United States' particular reliance upon space-based capabilities, it is logical to consider whether critical infrastructure designation could drive government and industry to address important issues facing the space sector.

“

The lack of comprehensive guidance, accountability mechanisms, and appropriate incentives to drive the adoption of cybersecurity standards to protect space assets places the space sector at significant risk, whether from U.S. adversaries or unanticipated crises.

Two pending policy and legislative initiatives are currently addressing improved resilience of both space systems and previously designated critical infrastructure sectors. In June 2021, Congressman Ted W. Lieu (D-CA) and Congressman Ken Calvert (R-CA) introduced the *Space Infrastructure Act,* which would direct the designation of space systems, services, and technology as critical infrastructure.[9] The bill would direct government agencies to develop guidance on how to protect spacecraft and launch vehicles, ground systems, and launch infrastructure, related production facilities, and information technology systems. In addition, a review is underway of Presidential Policy Directive 21 (PPD-21), a 2013 document that identifies critical infrastructure sectors and lead agencies in order to promote resiliency of essential functions.[10]

REASONS TO DESIGNATE SPACE SYSTEMS AS CRITICAL INFRASTRUCTURE

The expanding scope of space activities has made space-based systems increasingly essential. In the national security realm, the government – and particularly the Intelligence Community – relies heavily on space systems built and deployed by commercial companies. Satellites recently deployed by commercial space companies have detected new intercontinental ballistic missile (ICBM) sites in China,[11] provided insights to aid disaster response,[12] revealed indicators of potential clashes along the India-Pakistan border,[13] tracked pirates and wildlife poachers,[14] and monitored illegal fishing activities in protected waters.[15] Other national security missions include intelligence collection, disaster prevention and preparedness, search and rescue, weather forecasting, remote sensing, and communications. Commercial geospatial capabilities are so critical and comprehensive that, as a senior NGA official announced at INSA's Intelligence and National Security Summit in September 2021, the agency plans to revise its 2018 Commercial GEOINT Strategy to direct that analysts use commercial information as primary sources of intelligence before turning to classified government assets.[16]

Space systems are also essential for many civilian applications. New, space-based 5G networks consisting of thousands of low earth orbit satellites will link to global cloud infrastructures, offering new hyperscale information infrastructures. Other commercial offerings include space-based imagery, transportation, resource mapping, enhanced navigation, and global connectivity for Internet of Things (IoT) devices. As these functions grow in importance to national security and economic activity, designation of space as critical infrastructure will help assure access to space and the resiliency of space systems.

The uniqueness and ubiquity of the space sector should also factor into the decision for designation. An examination of the U.S. Department of Homeland Security's National Critical Functions list[17] reveals that almost all essential functions depend on space systems. Just to cite a few examples:

- Space systems are vital for agricultural transportation. The navigation of large agricultural machines on our nation's farms and fields depend on the Global Positioning System (GPS) satellite network.
- The discovery of new energy sources relies on the use of space-based imagery and sensing.
- 5G communication and information processing in rural areas will benefit from advanced space-based communication technology.

While some of these functions are covered by other designated critical infrastructure sectors (such as agriculture, energy, and telecommunications), no overall framework exists for space systems, leaving aspects of the space systems sector – including manufacturing, supply chain, and launch and operations services – without critical infrastructure support.

REASONS TO DEFER DESIGNATION OF SPACE SYSTEMS AS CRITICAL INFRASTRUCTURE

Due to the critical role space systems play, a great deal of overlap exists between the space sector and other critical infrastructure sectors. Designation of space may duplicate the mission of other Information Sharing and Analysis Centers (ISAC), creating cumbersome redundancies in information sharing processes. Under the umbrella of Critical Infrastructure Protection (CIP), the Department of Defense addresses space as part of its CIP responsibility through the mission of United States Strategic Command (USSTRATCOM).

The space sector may benefit from the designation of existing critical infrastructure sectors, such as agriculture, communications, information technology and energy, that depend on and include some space systems. To the extent that space systems support and are part of the Defense Industrial Base (DIB), initiatives to strengthen the security of the DIB should also improve the security of the space systems sector.

Despite this overlap with other critical infrastructure sectors, space assets cannot be properly protected by sector-specific measures that address space capabilities in a piecemeal fashion. The space sector's role in so many components of the U.S. economy and national security environment argue for steps to ensure the protection and resilience of the entire national space infrastructure.

BENEFITS OF A DESIGNATION

Designation of space systems as critical infrastructure would enhance the security and resiliency of essential space assets by generating several key outcomes. Designation would:[18]

1. Foster and strengthen intra-industry and government/industry collaboration. Designation would serve as a forcing function to clarify various government agencies' roles and responsibilities. Identifying which organizations should lead space-related security and resilience initiatives would lead to stronger strategic planning, closer interagency cooperation, and the allocation of resources to support space infrastructure protection initiatives.
2. Accelerate development of best practices and technologies for ensuring safety and resilience, particularly as new systems are being designed.
3. Enable the United States to establish a national-level Office of Primary Responsibility (OPR) with authority and resources to drive interagency efforts.
4. Telegraph to adversaries that the United States intends to defend critical space systems.
5. Organize a national community of stakeholders committed to assuring the protection and resiliency of space systems.
6. Promote global consensus regarding the criticality of these systems and the need for protection and sustainment, contributing to norms of behavior that designate certain space systems – particularly those related to civilian functions – as illegitimate targets for attack or disruption.
7. Identify a baseline assessment of threats to space assets, which would facilitate risk-based security and resiliency solutions by industry and government agencies at all levels.

“Identifying which organizations should lead space-related security and resilience initiatives would lead to stronger strategic planning, closer interagency cooperation, and the allocation of resources to support space infrastructure protection initiatives .

DESIGNATION WOULD FACILITATE GREATER INFORMATION-SHARING

The potential for greater public-private collaboration on threat assessments, vulnerability evaluations, and risk mitigation merits special examination, as no measures to enhance space resiliency can succeed without cooperation among the government agencies that evaluate adversary threats and the private entities that design, build, and operate space assets.

The Space Information Sharing and Analysis Center (Space ISAC), an all-threats information source for public and private entities in the space sector, serves as a trusted communication and analysis mechanism for space industry stakeholders to share threat and vulnerability information. By facilitating information sharing and developing timely, customized analysis, the Space ISAC supports response, mitigation, and resiliency initiatives.

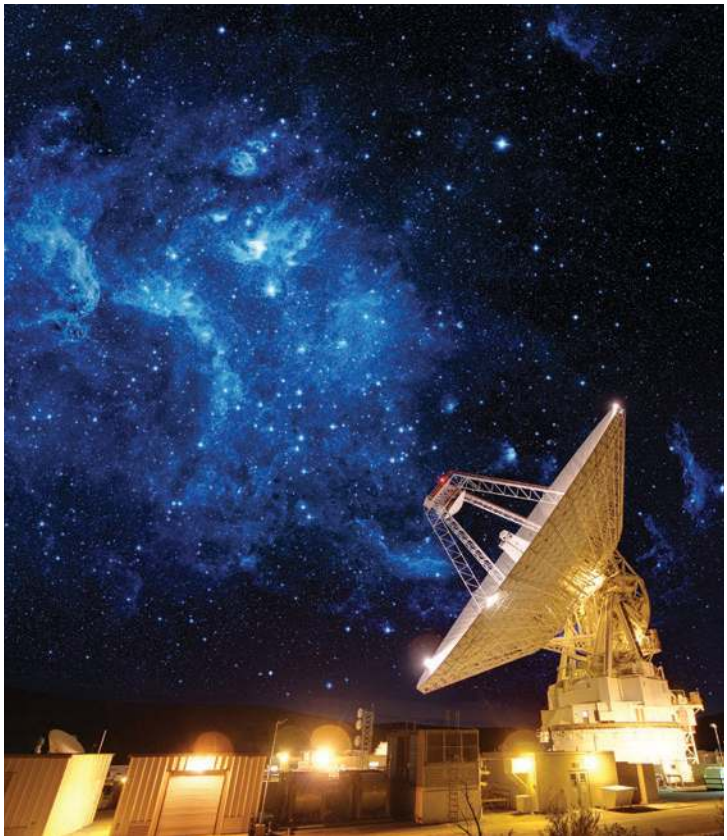
The designation of space as critical infrastructure would also engage additional potent information-sharing and intelligence resources supporting critical infrastructure sectors, such as the National Network of Fusion Centers (NNFC) and the 80 individual Fusion Centers around the country.[19] Fusion Centers are "owned and operated by state and local entities and serve as the primary focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information" for Federal, State, Local, Tribal, and Territorial (SLTT), and private sector partners.[20] Fusion Centers maintain contact with infrastructure sector experts and facilitate collaboration with DHS, FBI, and local law enforcement and emergency management.

As space-related applications and technologies become ubiquitous, local insights should provide valuable context for policymakers and space infrastructure operators. The NNFC and its constituent Fusion Centers help address information needs and gaps by injecting local reporting, suspicious activity, analysis, and subject matter expertise into the national information sharing environment on critical and complex topics, such as space. According to the Department of Homeland Security, Fusion Centers serve a critical infrastructure protection role by publishing products that "help customers understand the local implications of national intelligence, thus helping state and local officials better protect their communities and helping private sector partners protect their facilities and operations."[21]

The Justice Department's Foundational Baseline Capabilities guidance for the NNFC helps Fusion Centers "establish a critical infrastructure and key resources (CIKR) protection analytic capability that supports infrastructure security activities at the state and local levels."[22] Fusion Centers have extensive experience sharing, fusing, and analyzing information related to critical infrastructure. Designating space as a critical infrastructure sector would therefore provide the space sector with the capability for broader information sharing through the NNFC and similar entities.

Designation would facilitate several types of collaboration:

- **Broad sharing of space-related information and region-specific expertise.** Because a great deal of critical infrastructure, including space-related infrastructure, is owned by the private sector, engagement with space stakeholders at the state and local level is critical to identifying and sharing threats, vulnerabilities, and suspicious activity in the communities of those who know them best. Fusion Centers collaborate with local private sector partners, including those who manage and own infrastructure assets, to provide analytic products and intelligence necessary to mitigate threats and vulnerabilities. These products are accessible via the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) community of interest and other mechanisms that facilitate sharing of products and information with participating partners. In addition, local space subject matter experts could provide insights to Fusion Center analysis and reporting, thereby providing the national information sharing environment reports on suspicious activity and changes in space-related trends and adversary capabilities.



– **Partnership among the National Network of Fusion Centers, ISAOs, ISACs, and other agencies, particularly regarding cyber threats.** The Department of Justice recommends Fusion Centers work with Information Sharing and Analysis Organizations (ISAO) and Information Sharing and Analysis Centers (ISACs), particularly the Multi-State ISAC (MS-ISAC), to "develop and implement plans to coordinate cyber information and intelligence sharing."[23] Designating space as a critical infrastructure would strongly encourage the NNFC to create plans and mechanisms to engage ISAOs, ISACs, and subject matter experts on cyber and physical threats to space-related systems. This would enable a wider information-sharing network for local threats, vulnerabilities, intelligence reporting, subject matter expertise, and suspicious activity.

– **Greater general awareness of threats, vulnerabilities, and corrective action.** The NNFC provides partners with threat intelligence and vulnerability information, as well as guidance on incident prevention, protection, response, and recovery. Serving as a two-way information-sharing mechanism, the NNFC provides partners with up-to-date indicators of suspicious activity related to each critical infrastructure sector, and partners provide threat and vulnerability information in response. For example, if space was a designated critical infrastructure, the federal government and NNFC might partner to publish an unclassified product like "Indicators of Suspicious Activity Related to Space Infrastructure and Assets" for dissemination to state and local partners based on the latest tactics, techniques, procedures, and intelligence reporting of adversaries targeting space-related resources. While select partners have access to classified information through Fusion Centers when warranted, Fusion Centers manage established tear line and downgrade processes to enable wide dissemination of reports based on classified intelligence. The result would be local-level reporting and information sharing related to current and future threats and vulnerabilities in the space sector, which may mitigate security risks by revealing space-related adversary intent, capabilities, and activities.

> "...engagement with space stakeholders at the state and local level is critical to identifying and sharing threats, vulnerabilities, and suspicious activity in the communities of those who know them best.

- **Analysis and case studies for the broader community.** The NNFC produces impactful reporting and analysis on a broad range of topics related to critical infrastructure protection. A standing strategy for the NNFC is to publish analytic products relevant to local infrastructure providers and stakeholders. With space as a designed critical infrastructure sector, the NNFC would have a greater awareness of needs and requirements for space and produce more relevant documents to state and local space stakeholders.
- **Additional activities.** A critical infrastructure designation could enable additional forms of public-private collaboration on space-related matters. For example, the Space ISAC is already conducting a series of tabletop exercises focused on space assets' cyber resilience; a cyber test range for commercial space systems could be a logical next step following those exercises. The Space ISAC is exploring the "tear line question"—that is, what additional information might be shared by space systems enterprises under emergency conditions. Newer indication and warning guidelines can be developed given broader stakeholder engagement and recognition of space systems' importance.

CONCLUSION

The growth and importance of the space sector, its burgeoning complexity (manufacturing, launch, operations, etc.), links with other sectors, and increasingly vital role within our national economy and way of life all argue for the designation of space as a critical infrastructure sector. Active and sustained public-private partnership can mitigate threats to space-related capabilities and drive the development of best practices and technologies needed to strengthen space systems' security and resilience. As the nation's dependence on space systems intensifies, so does the need to secure these systems. The designation of space as a critical infrastructure sector, and the government-industry collaboration it would foster, would promote both national and economic security.

REFERENCES

[1]Nibedita Mohanta, "How many satellites are orbiting the Earth in 2021?," Geospatial World, May 28, 2021. At https://www.geospatialworld.net/blogs/how-many-satellites-are-orbiting-the-earth-in-2021/. The number of satellites may in fact be far higher, if one includes microsats and satellites no longer operational. See https://maps.esri.com/rc/sat2/index.html.

[2]Michael Sheetz, "Bank of America Expects the Space Industry to Triple to a $1.4 Trillion Market Within a Decade," CNBC.com, October 4, 2020. At https://www.cnbc.com/2020/10/02/why-the-space-industry-may-triple-to-1point4-trillion-by-2030.html.

[3]Cybersecurity and Infrastructure Security Agency, National Critical Functions Set, website. At https://www.cisa.gov/national-critical-functions-set.

[4]John D. Hill, Performing the Duties of Assistant Secretary of Defense for Space Policy, remarks at the 36th Space Symposium, August 24, 2021. At https://www.defense.gov/Newsroom/Speeches/Speech/Article/2747709/remarks-of-mr-john-d-hill-performing-the-duties-of-assistant-secretary-of-defen/.

[5]National Space Council, "Cybersecurity Principles for Space Systems," Space Policy Directive-5, September 4, 2020. At https://history.nasa.gov/SPD-5.pdf.

[6]See, for example, Aspen Cybersecurity Group, "Securing the Internet's Public Core," December 2, 2020. At https://www.aspeninstitute.org/longform/a-national-cybersecurity-agenda-for-resilient-digital-infrastructure/securing-the-internets-public-core/.

[7]National Air and Space Intelligence Center, Competing in Space, December 2018, pp. 4-5. At https://www.nasic.af.mil/Portals/19/documents/Space_Glossy_FINAL--15Jan_Single_Page.pdf.

[8]Michael Bartok, et. al., "Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services," NISTIR 8323, February 2021. At https://csrc.nist.gov/publications/detail/nistir/8323/final. See also The White House, "National Space Traffic Management Policy," Space Policy Directive-3, June 18, 2018. At https://trumpwhitehouse.archives.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/.

[9]"Reps Lieu and Calvert Introduce Bill to Designate Space as Critical Infrastructure," press release, June 4, 2021. At https://lieu.house.gov/media-center/press-releases/reps-lieu-and-calvert-introduce-bill-designate-space-critical. See also Jeff Foust, "House Bill Would Designate Space as Critical Infrastructure," Space News, June 4, 2021. At https://spacenews.com/house-bill-would-designate-space-as-critical-infrastructure/. For the bill text, see H.R. 3713, 117th Cong., 1st sess. At https://www.congress.gov/117/bills/hr3713/BILLS-117hr3713ih.pdf.

[10]The White House, Critical Infrastructure Security and Resilience, Presidential Policy Directive 21 (PPD-21), February 12, 2013. At https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[11]Ryder Kimball, "China's Nuclear Missile Silos, Flash Floods in the Himalayas, and an Obituary for the Spruce," Planet, July 26, 2021. At https://www.planet.com/pulse/chinas-nuclear-missile-silos-flash-floods-in-the-himalayas-and-an-obituary-for-the-spruce/

[12]Malia Politzer, "Harnessing Satellite Data for Pandemic Response: Lessons from COVID-19," Devex, October 26, 2020. At https://www.devex.com/news/harnessing-satellite-data-for-pandemic-response-lessons-from-covid-19-98382

[13]Bryan Bender, Politico Space, April 23, 2021. At https://www.politico.com/newsletters/politico-space/2021/04/23/the-space-industrys-david-vs-goliath-492571.

[14]Cody DeBos, "HawkEye 360 to Launch Pirate-Hunting Satellites into Orbit," The Burn-In, July 17, 2020. At https://www.theburnin.com/startups/hawkeye-360-launch-pirate-hunting-satellites-spacex-2020-07-17/.

[15]"Small, Cheap Spy Satellites Mean There's No Hiding Place," The Economist, March 18, 2021. At https://www.economist.com/science-and-technology/2021/03/18/small-cheap-spy-satellites-mean-theres-no-hiding-place.

[16]Justin Doubleday, "New GEOINT Strategy Will Direct Agencies to Look at Commercial Services First," Federal News Network, September 16, 2021. At https://federalnewsnetwork.com/contracting/2021/09/new-geoint-strategy-will-direct-agencies-to-look-at-commercial-services-first/.

[17]Cybersecurity and Infrastructure Security Agency, National Critical Functions, website. At https://www.cisa.gov/national-critical-functions.

[18]See, for example, an opinion column by two founding members of the Space Information Sharing and Analysis Center (ISAC) Board of Directors: Edward Swallow and Samuel Visner, "It's Time to Declare Space Systems as Critical Infrastructure," Politico, April 2, 2021. At https://www.politico.com/news/2021/04/02/its-time-to-declare-space-systems-as-critical-infrastructure-478848.

[19]For a listing of all 80 Fusion Centers, see National Network of Fusion Centers, website. At https://nfcausa.wpengine.com/fusion-centers/.

[20]Department of Homeland Security, Fusion Centers, website. At https://www.dhs.gov/fusion-centers.

[21]Cybersecurity and Infrastructure Security Agency, Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community, October 2016, p. 25. At https://www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf.

[22]Department of Justice, Critical Infrastructure and Key Resources (CIKR) Protection Capabilities for Fusion Centers, December 2008, p. 1. At https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/CIKR%20protection%20capabilities%20for%20fusion%20centers%20s.pdf.

[23]Department of Justice, Cyber Integration for Fusion Centers, May 2015, pp. 7-8. At https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/cyber_integration_for_fusion_centers.pdf.

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to this paper.

INSA MEMBERS

Jim Keffer, *Chair, Cyber Council*

Steve Orrin,
Vice Chair, Cyber Council

Tyler Farrar

Adam Golodner

Jeremy Harchelroad

Dan Johnson

Marc Kolenko

Al Munson

Patricia Schouker

Jason Swope

Samuel Visner

Jennifer Walsmith

INSA STAFF

Suzanne Wilson Heckenberg, *President*

John Doyon, *Executive Vice President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor,
Director of Communications and Policy

Britany Dowd,
Marketing and Communications Assistant

Rachel Thompson, *Fellow*

Harry Brooks, *Intern*

Samantha Juarez, *Intern*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. INSA's 160+ member organizations and 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

ABOUT INSA'S CYBER COUNCIL

INSA's Cyber Council seeks to fuse knowledge from industry, government, and academic experts in order to provide authoritative and influential insights regarding the national security challenges present in the cyber domain. The Council works to promote a greater understanding of cyber threats, challenges, and opportunities that can be addressed effectively through public-private collaboration.

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Building a Stronger Intelligence Community