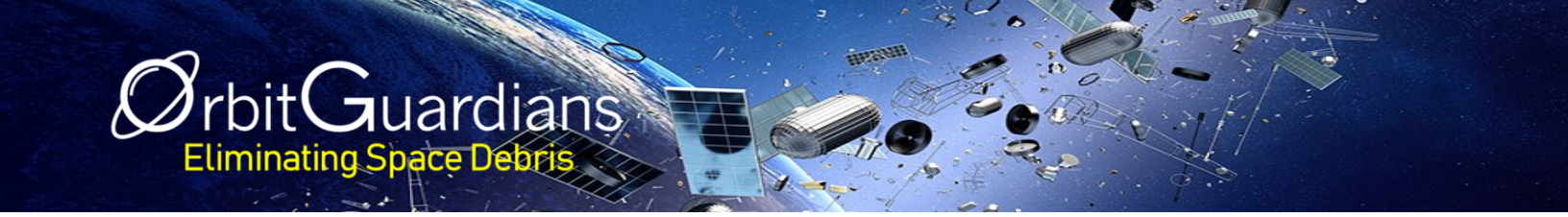


October 28, 2021

A Critical Look at DHS and Orbital Debris

The DHS mission to safeguard America, her people, and our values is weakening as the lack of satellite system protection neglects the emerging risk of orbital debris.

Laying the Foundation

The Homeland Security Act of 2002 was a direct result of the 9/11 terrorist attack upon the United States, which began operation of the Department of Homeland Security (DHS) in 2003. The DHS mission is bound to its ability to protect our critical infrastructure and key resources (CIKR), as defined in the 2006, 2009, and 2013 National Infrastructure Protection Plan (NIPP), though satellites have *yet* to be explicitly identified as critical infrastructure.

Space enthusiasts have long been aware of the risk orbital debris brings to our infrastructure and our way of life. The underlying problem is not designing solutions to solve the problem, but rather figuring out who and how to pay for the solution. Many think the government, Space Force, NASA, DoC, NOAA, FAA, etc. should be leading the way for Space Traffic Management (STM) and Active Debris Removal (ADR) services, but historically, they have been slow to provide direction in many sectors of the government. Let's look at DHS regarding protection of our space critical infrastructure.

According to the 2013 NIPP Executive Summary,

> Within the context of the risk, policy, and operating environments, critical infrastructure sector and cross-sector partnership structures provide a framework to guide the collective efforts of partners. The national effort to strengthen critical infrastructure security and resilience depends on the ability of public and private critical infrastructure owners and operators to make risk-informed decisions when allocating limited resources in both steady-state and crisis operations.

The green text says DHS should provide a framework to guide efforts, yet the very next sentence provides operators a loophole of "depends on the ability… to make informed decisions".

The NIPP categorizes a framework list of Critical Infrastructure Sectors (or Nation Critical Functions) and defines these critical infrastructure sectors as so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health of safety, or any combination thereof.

In the same document, the Critical Infrastructure Operating Environment states that position, navigation, and timing (PNT) services are critical to operations across multiple sectors and are vital to incident response.

> located infrastructure, such as water and electric lines running under a bridge span). Interdependencies may be limited to small urban or rural areas or span vast regions, crossing jurisdictional and national boundaries, including infrastructure that require accurate and precise positioning, navigation, and timing (PNT) data. PNT services are critical to the operations of multiple critical infrastructure sectors and are vital to incident response.

Yet, as with all the sectors, inadequate expenditures on operation and maintenance have allowed the infrastructure to deteriorate.

> owners and operators. Much of the critical infrastructure community continues to integrate cybersecurity into core business practices, making significant investments to increase security and resilience. In other areas, however, despite public and private sector expenditures to operate and maintain critical infrastructure systems, the level of investment has not been adequate, as evidenced by the deteriorating condition of many infrastructure systems. The National Academy of Sciences reported that the Nation's earlier heavy investment in the design, construction, and operation of critical infrastructure systems—water, wastewater, energy, transportation, and telecommunications—has not been matched with the funds necessary to keep these systems in good condition or to upgrade them to meet the demands of a growing and shifting population.[8]

While space assets, including PNT (GPS), are not part of the CIKR, it is not difficult to understand that the orbital debris environment has and will get worse over time. In fact, NASA has tracked over 400 events that have generated over 100 million debris objects orbiting Earth.

Who is Responsible for Orbital Debris?

From the 2013 NIPP, Appendix B. Roles, Responsibilities, and Capabilities of Critical Infrastructure Partners and Stakeholders, for CIKR owners and operators the risk versus consequence (of what?) tradeoffs are based upon what is known about the risk environment and what is economically justifiable and sustainable.

> For many private sector enterprises, the level of investment in security reflects risk-versus-consequence tradeoffs that are based on two factors: (1) what is known about the risk environment, and (2) what is economically justifiable and sustainable in a competitive marketplace or within resource constraints. In the context of the first factor, the Federal Government is uniquely positioned to help inform critical infrastructure investment decisions and operational planning across the sectors. Owners and operators may look to the government and information sharing and analysis organizations like ISACs as a source of security-related best practices and for attack or natural hazard indications, warnings, and threat assessments.

What the operators know about the risk environment is based upon CIKR risk assessments and response planning which they "***MAY***" decide to perform, as shown below.

> Within this diverse landscape, critical infrastructure owners and operators may contribute to national critical infrastructure security and resilience efforts through a range of activities. These activities may include but are not limited to: performing critical infrastructure risk assessments; understanding dependencies and interdependencies; developing and coordinating emergency response plans with appropriate Federal and SLTT government authorities; establishing continuity plans and programs that facilitate the performance of lifeline functions during an incident; participating in critical infrastructure-focused training and exercise activities with public and private sector partners; and contributing technical expertise to the critical infrastructure security and resilience efforts of DHS and the SSAs.

The NIPP specifies that key initiatives, milestones, and metrics are required to achieve the Nation's CIKR protection mission. The cornerstone of the NIPP is its risk management framework, which is essentially supposed to assess national or sector risk. In fact,

the Communication Sector's approach to network defense prioritizes…

> sector-specific risks and interdependencies. Consistent with the NIPP 2013 Critical Infrastructure Risk Management Framework, the Communications Sector's approach to network defense prioritizes assets, assesses threats and vulnerabilities, and then uses the findings of these assessments as criteria to focus resources on defenses that yield optimal protection. The Communications Sector regularly undertakes risk assessments to address evolving issues by topic, segment, or threat. Across the Communications Sector, industry and government partners collaborate to conduct risk assessments as an ongoing activity, with the intent to maintain a national communications infrastructure that is resilient, diverse, redundant, and recoverable.

However, what are the chances of infrastructure protection when 85% of satellites are owned by private industry and most of the council membership? Let's discover who oversees the unrecognized critical space infrastructure.

Partnership Structure

Understanding the partnership structure within each sector is paramount to recognizing how priorities and requirements are reported to the President for budget submission. To grasp this appreciation, let's highlight the communications sector, because it is the only sector that identifies satellites as a sub-sector. Their Communications Sector Partnership Model is laid out in their 2015 Communications Sector-Specific Plan (CSSP), as follows:

- Industry
  - National Security Telecommunications Advisory Council
  - Communications SCC
  - Communications ISAC
- Government
  - Emergency Operating Plan
  - Communications GCC
  - Communications National Coordinating Center

The above list of industry and government URLs point to the About Us, Charter, or Membership pages for each partner. Of particular interest are the members of these partnerships. This is where is gets interesting, so bear with me.

The Communications SCC was established in 2005, with membership that includes private owner/operators, trade associations, and standards bodies. For instance, the Satellite Industry Association (SIA) is a 501(c)(6) organization that promotes its members' interests *without* the goal of making a profit. They *advocate industry position* with Capitol Hill policy makers, the White House, FCC, and key Executive Branch departments and agencies regarding policy around space debris, mitigation, and sustainability. SIA also organizes the Space Safety Working Group (what are they working on?) and participates as a member of the Global Satellite Coalition, whose mission is to ensure the future for millions of global stakeholders who depend on satellite-based solutions.

Where are the academic, NASA, USSF, DoC, STM, ADR partnership representatives?

Like the 2013 NIPP, the CSSP also states that a partial or complete loss of key fiber optic, coaxial, *satellite*, and/or microwave trunks could lead to loss of Internet routing, access, and connection service functions. These disruptions could cut off key long-haul, high-capacity Internet trunks that could isolate civil, defense, and commercial users who depend on these connections. Dependencies were also cited for the banking and finance sectors and the federal government.

Interestingly, the Space Information Sharing and Analysis Center (Space ISAC) was founded 14 years later in 2019. Initially sponsored by NASA, USSF, and NRO, the public and private representatives have spoke of the importance of protecting critical space assets. Unfortunately, space systems have not made it into the CIKR list.

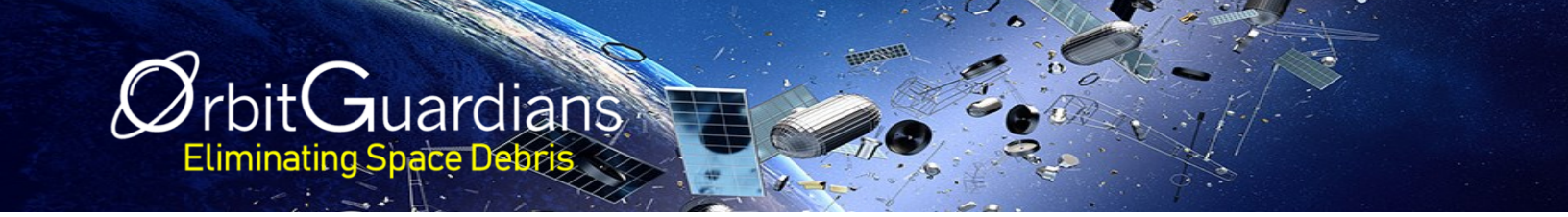
In 2021, CISA launched the Space Systems Critical Infrastructure Working Group as a mix of government and industry members that will identify and develop strategies to minimize risks to space systems that support the nations critical infrastructure. Published agendas provide no meeting details, meeting minutes, action items, or future topics around identifying space systems as CIKR.

So, if NSTAC is not identifying, evaluating, or prioritizing the risks of orbital debris, it makes sense that neither the National Risk Management Center nor the Communications Sector Risk Management Agency are engaged with assessing, planning, or controlling the orbital debris risk.

Vulnerability Assessments

The 2011 Strategic National Risk Assessment supports Presidential Policy Directive 8 to create a National Preparedness Goal, a National Preparedness System, and a National Preparedness Report. As foundational elements of the NIPP, vulnerability assessments are voluntary and nonregulatory. CISA Protective Security Advisors (PSA) offer assessments *at the request* of critical infrastructure owners and operators.

Since space assets are not identified as critical infrastructure, vulnerability assessments do not officially fall under the prevue of the PSA program. Without satellite operators requesting vulnerability assessments, of course the NSTAC report to the President excludes budgetary requirements to protect our country's space assets. Why has orbital debris escaped DHS scrutiny?



The Fox Guarding the Hen (White) House

It's no surprise that there is a lack of action regarding the increasing risk of orbital debris.

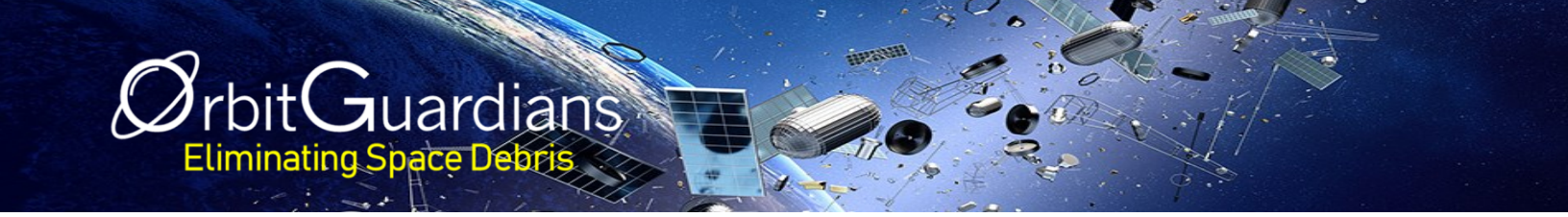
- The 2008 NSTAC Report to the President on Commercial Communications on the GPS neglected to mention orbital debris or collisions as a risk.
- The 2009 NSTAC Report to the President on Commercial Satellite Communications Mission Assurance did identify orbital debris as a *low* potential for collision with active satellites. This makes sense as more satellites capable of debris avoidance maneuvers have been launched. However, it neglects to discuss debris to debris collisions, of which there would be higher likelihood. Additionally, it recommended the Secretary of Defense make safety of flight and the preservation of the space environment a leading national security driver for enhanced space situational awareness efforts, which can be viewed as shifting the blame (responsibility) from satellite operators to the DoD.
- The 2017 DHS CISA National Risk Management Center report about GPS capabilities clearly identified precise PNT as a requirement for agriculture, port operations, consumer location-based services, and maritime navigation and that a 30-day loss of GPS would negatively affect the economy by $1 billion per day, which could be 50% higher if disruption occurred at an inopportune time.
- The 2019 NSTAC Factsheet does not list recent publications related to orbital debris.

NSTAC has identified potential resiliency stressors (i.e., electromagnetic pulse, solar flare, PNT disruption, long-term outage, supply chain cyber-attacks) for critical infrastructure sectors, but has not vigorously assessed orbital debris, which is an issue clearly identified as a concern across the satellite end-user community. Let us not forget the hierarchy shown in the Communications Sector Partnership Model above, where NSTAC is the partner responsible for advising the President of the United States. Is POTUS making budgetary decisions based upon omissive NSTAC reports submitted to the Oval Office?

Perhaps the Office of Management and Budget (OMB) needs to evaluate the effectiveness of the DHS role to improve its administrative management, performance measures and coordinating mechanisms, and reduce unnecessary burdens to the public. Afterall, OMB critical mission is to:

1. Develop and execute budgets, a prominent government-wide process managed from the Executive Office of the President (EOP) and a device by which a president implements policy, priority, and action in everything from the DoD to NASA.
2. Manage other agencies' financial, paperwork, and IT.

The fox (satellite industry) has lurked in the shadows to capture the eggs (massive profits) while the farmer (government) provides no oversight of the hen house (orbital commons), thus allowing the tragedy to grow out of control. It's no wonder the industry has no vested interest in pursuing satellite safety with vigor.



Closing

How could space infrastructure be left off the CIKR list? Perhaps it's time to declare space systems as critical infrastructure and include academia, NASA, USSF, DoC, STM, and ADR partners to the membership.

Orbital debris is imperceptibly growing while the United States government and industry have overlooked the danger to our future. NASA has cataloged over 400 events that have helped generate the estimated 100 million debris objects orbiting Earth. As 19% of the tracked debris reside in or transit through medium Earth orbit (MEO), the danger takes on a whole new perspective considering one-quarter of our nearly $22 trillion U.S. GDP is the direct result of GPS, which operates in MEO. Not to mention that within the next decade, 17 times more space missions are slated to launch as Space Force wants to outsource ADR and NASA OIG reports their agency lacks the initiative and leadership to develop or acquire ADR technologies.

American confidence in our usurped election infrastructure, as described in Devolution – Part 5, is a hit to our national security. Similarly, we must overcome our false sense of security pertaining to the effects of orbital debris. We must act according to the time value of money to:

- Support SPD-3 using STM Act of 2022 legislation for the Internal Revenue Service to implement tax incentivizes for financial contributions from satellite operators and taxpayers.
- Define and identify Orbital Carrying Capacity and Space Traffic Footprint.
- Perform orbital debris vulnerability assessment for the whole of the environment, including active satellites, defunct satellites, expended hardware, and small flotsam.
- Begin ADR development while STM comes online.

Without action the U.S. and the rest of the globe are on a disastrous trajectory, because while occurring on a slower time scale than a nuclear fission reaction, once an orbit exceeds its carrying capacity (reaches critical mass) a chain reaction of collisions will explode out of control. Are we so arrogant that we are waiting for another Chernobyl-type incident?