# Space ISAC Frequently Asked Questions

Current and Future Capabilities

*Visit s-isac.org for more information*

**Q: What specific threats to the space community is Space ISAC focused on addressing?**

**A:** Space ISAC's operational scope encompasses all threats and hazards affecting the global space community. Such threats include, but are not limited to, cyber activity, kinetic and non-kinetic threats to space systems, adversary capabilities, in-the-wild exploitation of vulnerabilities, targeted campaigns against critical infrastructure, etc. Our priorities continuously focus on the implications of these threats to multiple areas including operations technology, supply chain, business systems, and mission operations.

Space ISAC considers all segments of the space sector for information sharing; these segments are defined as:

**Link Segment:** Consists of signal transmission between the satellite(s) and the ground station

**Space Segment:** Consists of space assets (i.e constellation of satellites)

**Launch Segment:** Consists of the integrated launcher and the facilities needed for manufacturing, testing, and injecting payloads to their desired orbit

**Ground Segment:** Consists of a network of ground stations that generate navigation data to be uplinked to the satellites, and subsequently to be used by the user receiver for aiding in position consumption

**User Segment:** Consists of the outputs from space systems to the user

Specific threats to the space segments may include:

Link Segment

- Command Intrusion
- Malware/Ransomware
- Denial of Service
- Remote Code Execution
- Man in the Middle (MITM) Attack
- Spoofing/GPS Jamming

Space Segment

- GPS Interference
- Spoofing/Jamming
- Space Debris
- Space Weather Interference
- Anomalous behavior

Launch Segment

- Command Intrusion
- Denial of Service
- Remote Code Execution
- GPS Jamming
- Insider Threat

Ground Segment

- Industrial Control Systems/Operations Technology Attacks
- Supply Chain Attacks
- Malware/Ransomware
- Remote Code Execution
- Terminal Hacking/Hijacking
- GPS Interference

Effects to the User Segment

- Loss of Network Connectivity
- Compromised Banking Transactions
- GPS interference
- Supply Chain Disturbances
- Position, Navigation, and Timing (PNT) interference

**Q: What is Space ISAC doing to help members secure their systems?**

**A:** Space ISAC is routinely disseminating alerts and advisories from trusted members and partners that detail the current adversary activity ranging from unsophisticated hackers, advanced persistent threats (APT), or nation state actors. Members receive daily notices of cyber threats, incidents, and vulnerabilities to critical systems.

Many alerts contain indicators of compromise (IOCs), which members can use to scan networks for potential intrusions. Alerts may also contain details of the tactics, techniques, and procedures (TTP) used by threat actors, as well as recommendations for preventing and responding to threats, all helping members to secure their systems. Space ISAC maintains a list of priorities for information sharing, as well as a repository of known threat actors to aid in this process. In addition to regularly shared alerts, Space ISAC also sends out daily and weekly information products with the goal of increasing situational awareness.

**Q: What efforts are Space ISAC members implementing to increase their security posture?**

**A:** Members of Space ISAC have collectively increased their security posture regarding the range of global cyber threats. Specific efforts include, increased employee cybersecurity training, advanced internal and external monitoring of business operations networks, and applying additional precautions to guard points of entry and to identify intrusions. Space ISAC encourages implementing emerging frameworks such as: a Zero Trust Architecture approach, Defense in Depth, onboard intrusion detection, as well as increased collaboration with government agencies.

Space ISAC has distributed multiple requests for information (RFIs) to better understand what steps the community is taking to address an increased threat environment. Members are encouraged to provide feedback anonymously and share strategies with other member organizations to enhance the security posture of the space sector.

**Q: With the ongoing events, such as the Russian invasion of Ukraine, how is what Space ISAC is doing supporting its members through this time?**

**A:** Space ISAC is continuing to monitor for emerging threats to the space sector. Space ISAC is leveraging publicly available information and resources from members and partners to share actionable information to our trusted member base. Space ISAC's information sharing priority is to address both actual and potential attacks to space systems.

Space ISAC is aware of the surge of cyber activity precipitated by the Russian invasion of Ukraine and the potential target that space systems represent for adversarial cyber campaigns. In response to the surge of cybercrime, Space ISAC has published mitigation best practices, security recommendations, and insight on adversary tactics.

Space ISAC coordinates the dissemination of information through our Member Portal, where members send and receive secure alerts regarding recent cyber activity. Additionally, members have access to our

Threat Intelligence Platform (TIP) where users can review threat data such as malicious hashes, IPs, and exploited vulnerabilities. Space ISAC and our members are actively building a Watch Center that will continuously monitor global cyber events that affect space systems.

### Q: What role will the Space ISAC Watch Center play in preparing for potential cyber threats from nation state actors?

**A:** The Space ISAC Watch Center will provide an increased capability for collection, analysis, and dissemination of actionable information. Space ISAC will host analysts from private sector members and public sector entities in the Watch Center, where they will serve in an analytical role. The data sources shared within the Watch Center will allow for an increase in the collection of information, with feeds derived from all segments of the space sector. These contributions will assist greatly in analysis of information, resulting in more enrichment, better recommendations, and a more comprehensive understanding of trends. Lastly, the Watch Center will present an increased capability to disseminate information, engage in member inquiries, and respond to incidents in a timely manner.

### Q: How does Space ISAC plan to respond to future geopolitical events and in times of increased risk?

**A:** Space ISAC looks to increase its operational capability with the launch of our Watch Center, where our goal is to reach Initial Operating Capability by Q4 2022. Members will play a large role in achieving this goal as many are closely involved in the architecture design and preparation, as well as providing data sources and threat scenario use cases that demonstrate the value the Watch Center will bring to the global space community.

A larger interjection of data sources for aggregation and evaluation of threat data will allow Space ISAC to provide a more complete and accurate threat picture for absorption for the space community. Watch Center analysts will be able to identify threat actors and correlate tactics, techniques, and procedures (TTP) to space systems through the fusion of disparate data feeds. Regardless of the geopolitical landscape, the Space ISAC will continue to provide support to its members for the protection of assets. Should an event arise, the ISAC will be proactively vigilant to monitor the environment for new and emerging threats.