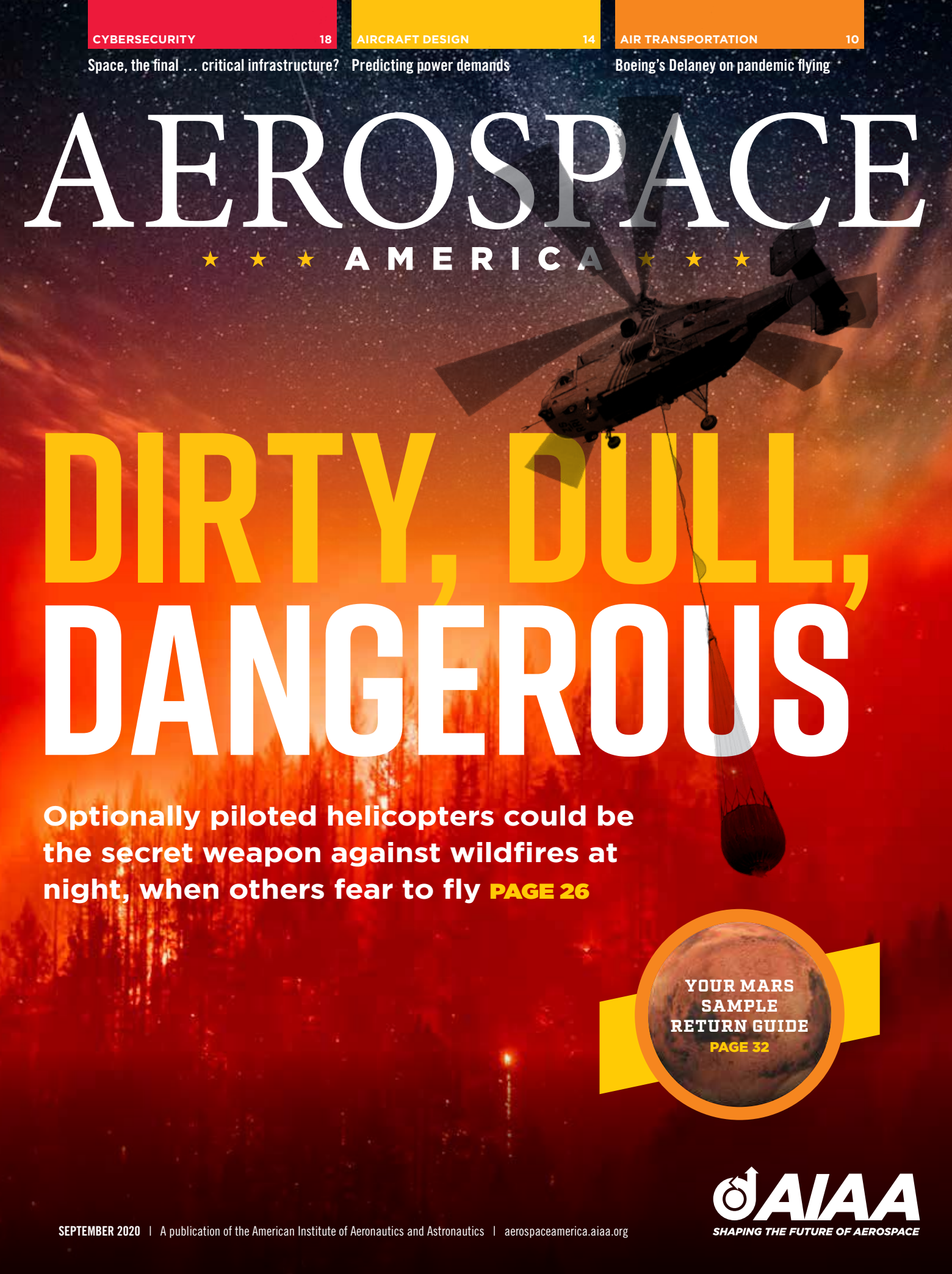
AEROSPACE
AMERICA



DIRTY, DULL, DANGEROUS

Optionally piloted helicopters could be the secret weapon against wildfires at night, when others fear to fly PAGE 26

YOUR MARS SAMPLE RETURN GUIDE
PAGE 32

SEPTEMBER 2020 | A publication of the American Institute of Aeronautics and Astronautics | aerospaceamerica.aiaa.org

AIAA
SHAPING THE FUTURE OF AEROSPACE

CYBER FOCUS: SPACE

The GPS constellation, communications satellites, the rockets that launch them, and the ranges and networks that control them have something in common. Under U.S. cybersecurity policy, they do not amount to a specific sector of critical infrastructure. The Trump administration may change this. Debra Werner finds out why.

BY DEBRA WERNER | werner.debra@gmail.com

It's been 12 years since the U.S. Department of Homeland Security designated a new critical infrastructure sector. Then-Homeland Security Secretary Michael Chertoff declared the U.S. manufacturing base as its own sector of critical infrastructure, encompassing everything from production of appliances to motor vehicles to aerospace parts and more. The declaration signaled that manufacturing was vital to U.S. national and economic security and, therefore, government agencies should be legally required to work together to safeguard it.

Now the Trump administration is considering whether space technology, equipment and facilities should receive the same critical infrastructure designation as 16 other sectors. The case for doing so is not as obvious as it might sound. Many satellites and rockets already receive the heightened attention afforded to critical infrastructure, though indirectly. Satellites that transmit phone calls, videos and data fall under the communications sector, and military satellites plus the rockets to launch them are part of the defense industrial base sector.

Even so, U.S. reliance on space infrastructure continues to grow, and some in the Trump administration think the risks warrant additional security scrutiny.

Nothing has been decided yet. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, or CISA, is evaluating various "courses of action to make sure that space infrastructure is getting the attention it needs from a national security and cybersecurity perspective," says CISA Assistant Director Bob Kolasky, who leads CISA's National Risk Management Center, an organization established in 2018 to pinpoint and address the most serious threats to critical infrastructure.

A Trump administration official made the case to me for such a declaration in an email approved by a spokesperson on the condition of anonymity: "In significant ways, the makeup of space-based infrastructure, the growth of industries surrounding such infrastructure, and the increasing complexity and dependency of the industry have changed the national risk landscape," this official said.

The conversation about better protecting space technology was prompted by the National Cyber Strategy of the United States of America. The document, signed in 2018 by President Donald Trump, calls for greater collaboration among U.S. government agencies, U.S. space companies, international government agencies and nonprofits in the face of "growing cyber-related threats to space assets and supporting infrastructure," noting their importance in "positioning, navigation, and timing" — a reference to GPS — "intelligence, surveillance, and reconnaissance; satellite communications; and weather monitoring."

Now, it's up to Acting Homeland Security Secretary Chad Wolf to determine whether adding space technology to the critical infrastructure list will promote that collaboration. The DHS secretary's authority to designate critical infrastructure stems from the Critical Infrastructure Information Act, part of the Homeland Security Act of 2002, signed by President George W. Bush after the Sept. 11, 2001, terrorist attacks when officials worried that the next big assault might not begin as a physical one. U.S. law defines critical infrastructure as physical and cyber entities so vital that their incapacity or destruction "would have a debilitating impact on security, national economic security, national public health or safety."

Whether or not space technology is added to the critical infrastructure list, the Trump administration is well aware of its significance.

"For over a decade, national security strategies have recognized that space systems are essential to our prosperity, security and way of life," says the Trump administration official. "The expansion of commercial space interests demands closer coor-

▲ **Rocket engines** and their factories could become part of the U.S. critical infrastructure, a designation that could result in greater protection from cyber and physical threats because of their roles in launching national security satellites. Here, nozzles for Blue Origin's BE-4 at its factory.

Blue Origin

▶ **United Launch** Alliance's Atlas V Centaur upper stages, one of which is shown in ULA's Alabama factory, could soon begin launching astronauts for NASA. Declaring space technology as a critical infrastructure could improve their cybersecurity, some experts say.

United Launch Alliance

dination among critical infrastructure partners collectively to identify priorities to achieve security and resilience in space, not purely from the perspective of national defense, but also from the perspective of industry and commercial resilience in space and on the ground."

The GPS satellites, NASA scientific research missions and rocket launch sites are critical to U.S. national and economic security, says Kolasky, the risk center director. "The conversation right now is: Does it make sense to cleave off a space-focused critical infrastructure sector?"

Creating a new sector

If DHS decides it does, the agency would have to determine exactly what to include in the category. The easy calls would be satellite and rocket manufacturing facilities, launch sites and ground stations that send commands to satellites and retrieve data. But what about component and subcomponent suppliers or thermal vacuum chambers for satellite instrument testing?

Once the sector is defined, DHS would designate a sector-specific agency, meaning a government agency to act as an intermediary between sector representatives and other government agencies like the FBI that are on the lookout for physical or cyber threats. The sector-specific agency would then work closely with owners and operators of space technology, facilities and networks to establish standards, identify vulnerabilities and respond to cybersecu-

▲ **Spaceport America,** the commercial spaceport in New Mexico. The facility's cyber and physical security would receive additional U.S. government scrutiny if space were designated critical infrastructure.

Spaceport America

rity incidents, meaning any attempt to breech a network whether or not it succeeds.

The Treasury Department, for example, is the sector-specific agency for financial services. Treasury coordinates the work of local, state and federal government agencies in safeguarding private-sector banking and finance operations. It shares information with allies about threats through membership in the Financial Services Information Sharing and Analysis Center, or ISAC, which is based in Virginia with offices in the United Kingdom and Singapore.

"Banks and insurance companies are very competitive, but their top cybersecurity executives get together and share information," says Steve Lee, AIAA aerospace cybersecurity manager. "Because guess what, if Bank of America gets hacked or gets a ransomware attack, it's probably also happening to Chase Bank and Wells Fargo."

The space sector, though not viewed under U.S. policy as a category of critical infrastructure, does now have an ISAC associated with it. The Space ISAC was established last year at the National Cybersecurity Center in Colorado Springs, Colorado. Establishing this ISAC, however, was not necessarily a precursor to declaring space as a category of critical infrastructure. Aviation, for instance, has had its own ISAC since 2014 even though it falls under the transportation critical infrastructure sector.

Before the pandemic, Space ISAC members met repeatedly with DHS representatives and endorsed the idea of the designation. They pointed out the implications of a serious attack on "emergency

▶ **The security of the** GPS network is of special concern due to its role in banking, communications and more. GPS III satellites are shown at Lockheed Martin's processing center in Colorado.

Lockheed Martin

response, critical communications, weather, business operations and global and national security," Erin Miller, Space ISAC vice president of operations, explained in an email.

If the Trump administration were to designate space as critical infrastructure, companies would be freer to communicate with each other and with government agencies.

"Antitrust laws define the way companies are allowed to work together within a sector to prevent monopoly control," says Frank Backes, who leads the federal space and cybersecurity business units for Kratos Defense and Security Solutions, a government contractor and Space ISAC founding member based in San Diego. Once a sector is identified as critical infrastructure, the laws allow greater coordination to counter threats, adds Backes, Space ISAC board chair and president.

Sam Visner, a cybersecurity expert at MITRE Corp., one of the founding members of the Space ISAC, sees a broader impact. "Once something is regarded as critical infrastructure in this country, it provides sort of an ever-growing connective tissue for sharing threat intelligence and for sharing best practices," he says.

Rules governing critical infrastructure also afford companies flexibility in sharing information with government agencies on threats or incidents without incurring fines or penalties for any regulatory infractions.

"It's a structure that is pretty tried and true for ongoing collaboration between industry and government that sits outside of the general structure of where industry and government traditionally work together, which is a more heavily bureaucratic process," Kolasky adds. "This enables tight collaboration in some sectors on an almost daily basis."

Space industry executives told me they would welcome additional government collaboration and attention.

Government agencies devote considerable time and attention to investigating cyber and physical threats to critical infrastructure and enhancing defenses. Although some space assets fall within

U.S. critical infrastructure sectors

Critical infrastructure means "systems and assets, whether physical or virtual, so vital to the United States that the incapacitation 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," according to the Critical Infrastructure Protection Act of 2001.

Here is the current list:

- Chemical
- Commercial facilities
- Communications
- Critical manufacturing
- Dams
- Defense industrial base
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Government facilities
- Healthcare and public health
- Information technology
- Nuclear reactors, materials and waste
- Transportation systems
- Water and wastewater systems

▲ **The anechoic test** chamber at Lockheed Martin's GPS III Processing Facility in Colorado, where the company builds GPS satellites.

Lockheed Martin

existing critical infrastructure categories, GPS doesn't fit well in any of the categories.

Even satellite communications, which falls within the communications category, does not get as much attention as it would in a space-focused sector. "There's a lot of expertise in cybersecurity work done on terrestrial networks," Backes says. "There is much less focus on space communications networks."

Tangible and intangible benefits

If the declaration were made, the sector-specific agency would work with companies and agencies like the U.S. National Institute of Standards and Technology to adopt formal security rules.

"Creating standards and processes and procedures to protect space assets from adversaries or natural disasters would be a good thing," says Chris Bogdan, senior vice president for the aerospace business at Booz Allen Hamilton, another Space ISAC founding member. He notes, though, that some space companies may oppose the adoption of standards out of concern about the cost and time required to implement and maintain them.

Some arguments in favor of adding space to the critical infrastructure list are less tangible.

Declaring space a critical infrastructure would increase the stature and visibility of the sector, says Bogdan, a retired U.S. Air Force lieutenant general. "That's important because eventually we're going to have to invest a lot more on the federal, civil and commercial sides to protect it," he adds.

When a sector is designated critical infrastructure, the move has international implications as well. Adversaries recognize that the United States considers an attack on its critical infrastructure a significant attack, Kolasky says.

Allies, meanwhile, tend to join efforts to safeguard sectors declared critical infrastructure in the United States.

"I've had conversations with Germany, France, Japan and several other countries about space being identified as U.S. critical infrastructure," Backes says.

Moreover, the new label would highlight the growing importance of the commercial space sector and could prompt security steps akin to those the U.S. government takes to protect its satellites and space infrastructure. Designating something as critical infrastructure "benefits, first and foremost, the private sector which owns most of our nation's critical infrastructure," Visner says. A declaration like that "makes all of us take as seriously as we need to the job of defending it and making sure it operates safely." ★