NORTH DAKOTA STATE AND LOCAL INTELLIGENCE CENTER

CI/KR Ticker

July 9th, 2021

Included In This Summary

Click on the *section header* to go directly to that location in the summary.

TLP: WHITE

Sensitivity/ Handling Notice:
Sources may use **TLP: WHITE** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

NORTH DAKOTA AND REGIONAL

(U) FAA gives $2.3 million in Airport Improvement grants to North Dakota

(U) The U.S. Department of Transportation announced a total of $845 million in Airport Improvement Program grants across the country, including $2.3 million in grants to seven airports in North Dakota. Of those funds, Williston Basin International Airport received $510,840 towards updating XWA's airport master plan. "An up-to-date airport master plan is critical to ensure orderly long-term development," Airport Director Anthony Dudas told the Williston Herald. "Our current airport master plan was completed in 2016, which provided the blueprint for design and construction of XWA. Now that XWA is operational, it is important to update this plan to reflect any changes which occurred throughout construction as well as identifying our region's long-term goals for development of this critical piece of infrastructure."

Source: (U) https://www.willistonherald.com/faa-gives-2-3-million-in-airport-improvement

(U) North Dakota Sues Feds Over Oil, Gas Lease Sale Suspension

(U) North Dakota has sued the Biden administration over its suspension of new oil and gas leases on federal land and water, saying the move will cost the state hundreds of millions of dollars in lost revenue. The lawsuit filed in federal court in Bismarck claims the move is unlawful. It seeks to force the U.S. Bureau of Land Management to reschedule two lease sales that were canceled and block the agency from revoking others in the future. The lawsuit said the two canceled sales this year have cost the state more than $82 million.

Source: (U) https://www.breitbart.com/news/north-dakota-sues-feds-over-oil-gas-lease-sale-suspension/

(U) NDDOT Receives $16.75M to Construct Passing Lanes in First-ever INFRA Grant Award

(U) North Dakota Department of Transportation (NDDOT) has been awarded $16,750,000 to construct passing lanes along approximately 165 miles of US-52 between Carrington and Kenmare. This is the first award North Dakota has received through the Infrastructure for Rebuilding America (INFRA) grant program, an allocation inequity Senator Cramer has been using his position on the EPW Committee to try to fix.

Source: (U) https://www.devilslakejournal.com/nddot-16-750-000-construct-passing-lanes-first-ever-infra-grant

(U) North Dakota, Near Last in Electric Vehicles, Braces for New Market

(U) Home to just 266 registered fully electric vehicles, according to the state's Department of Transportation, North Dakota's tally is the lowest of any state. Fewer fully electric and plug-in hybrids have been registered here in the last 10 years than in any other state, according to the Alliance for Automotive Innovation, and last year, electric cars accounted for a smaller percentage of total vehicle sales in North Dakota than in all but one other state. But a spike in the number of charging stations over the last year may have sparked a turning point for EV accessibility in North Dakota.

Source: (U) https://www.inforum.com/North-Dakota-near-last-in-electric-vehicles-braces-for-new-market

NATIONAL

(U) Ransomware Hits Hundreds of US Companies, Security Firm Says

(U) A ransomware attack paralyzed the networks of at least 200 U.S. companies on Friday, according to a cybersecurity researcher whose company was responding to the incident. The REvil gang, a major Russian-speaking ransomware syndicate, appears to be behind the attack, said John Hammond of the security firm Huntress Labs. He said the criminals targeted a software supplier called Kaseya, using its network-management package as a conduit to spread the ransomware through cloud-service providers. Other researchers agreed with Hammond's assessment. "Kaseya handles large enterprise all the way to small businesses globally, so ultimately, (this) has the potential to spread to any size or scale business," Hammond said in a direct message on Twitter. "This is a colossal and devastating supply chain attack."

Source: (U) https://news.yahoo.com/ransomware-attack-paralyzes-hundreds-u-232413623.html

(U) NIST Releases Definition of Critical Software in Response to Cybersecurity Directive

(U) The National Institute of Standards and Technology last week released a definition of critical software, which the Cybersecurity & Infrastructure Security Agency will use to develop a list of critical software products, as directed by President Biden in a May executive order on improving U.S. cybersecurity. The AHA and Health Information Sharing and Analysis Center in April recommended health care leaders identify their organization's mission-critical third-party software and understand the potential cyber risk associated with these platforms to help prevent another "SolarWinds-like" cyberattack.

Source: (U) https://www.aha.org/nist-releases-definition-critical-software-response-cybersecurity

(U) CISA Releases "Bad Practices" with Hope of Decreasing Cyber Blunders

(U) The federal Cybersecurity and Infrastructure Security Agency (CISA) released a few cybersecurity "bad practices" this week to assist in decreasing the volume of knowable and preventable cyber mistakes. These bad practices are aimed at educating critical infrastructure owners and operators, as well as the defense industry and the organizations that support the supply chain for national critical functions. Any disruption, compromise, or degradation to these systems creates a national security threat so in addition to the list of best practices that the CISA has published, CISA aims to highlight some of the biggest cyber mistakes made by these entities.

Source: (U) https://www.natlawreview.com/article/cisa-releases-bad-practices-hope-decreasing-cyber-blunders

(U) Dragos & E-ISAC Announce Initiative to Bring ICS/OT Defense to Electricity Sector

(U) Dragos, Inc., a provider of cybersecurity for industrial controls systems (ICS)/operational technology (OT) environments and the North American Electric Reliability Corporation's (NERC) Electricity Information Sharing and Analysis Center (E-ISAC) have announced a joint initiative to strengthen collective defense and community-wide visibility for industrial cybersecurity in the North American electricity industry. The joint initiative enables E-ISAC analysts to gain greater visibility into industrial control system (ICS) cyber threats facing the electric sector through Dragos's Neighborhood Keeper technology. E-ISAC analysts will have the ability to view aggregate information about threat analytics and Indicators of Compromise (IOC) as they are detected within Neighborhood Keeper, and then share insights and trends gleaned from this information more broadly with all E-ISAC members, thus enabling the community to collectively defend itself against cyber adversaries.

Source: (U) https://www.dragos.com/dragos-e-isac-announce-initiative-bring-ics-ot-collective-defense-electricity

TLP: WHITE

Sensitivity/ Handling Notice:
Sources may use **TLP: WHITE** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

INTERNATIONAL

(U) Germany Denies Reports of Cyberattack On 'Critical' Infrastructure, Banks

(U) A cyberattack on German data service provider that works with government groups wasn't a part of a larger, more comprehensive attack, according to Bloomberg. The BSI Federal Cyber Security Authority said it denied the reports of the attack by Bild newspaper, which the paper said might be revenge against the international sanctions passed down against Russia. Bild said the group responsible was likely called "Fancy Lazarus," and had also referenced a group called "Fancy Bear" which Bloomberg writes was responsible for the hacking of Hillary Clinton's staff ahead of the 2016 election. According to Bloomberg, Fancy Lazarus had previously identified itself as Fancy Bear. The group has been involved in several "denial-of-service" attacks and have reportedly leveled the attacks against the energy, financial and insurance industries.
Source: (U) https://www.pymnts.com/germany-denies-reports-of-cyberattack-on-critical-infrastructure-banks/

(U) UN Official Warns Digital Technologies Open Areas for Attack

(U) The U.N. disarmament chief warned Tuesday that digital technologies are lowering barriers to malicious intrusions and opening potential areas for governments, armed groups, terrorists, and criminals to carry out attacks, including across international borders. Izumi Nakamitsu told a U.N. Security Council meeting on cybersecurity that there has been “a dramatic increase in the frequency of malicious incidents in recent years” ranging from disinformation to the disruption of computer networks which are contributing to “a diminishing trust and confidence” among nations.
Source: (U) https://www.claimsjournal.com/news/international/2021/07/01/304621.htm#

(U) Gov. Officials Ordered Use NIC Email for Communication Amid Chinese Cyberattacks

(U) Chinese hackers have been targeting India’s critical infrastructure like power grids which could cause widespread blackouts. And amid all this, the Union power ministry has ordered all government organizations under it to use “organization-specific email-ID” for all official communications. The Union power ministry sent out an office memorandum on June 22 that said - “The undersigned is directed to refer to the prevailing cyber vulnerability due to various cyber threats/malicious attempts made by hackers and to request that all organizations under the ministry of power ensure their officials use NIC email/organization-specific official email-id only for official communications."
Source: (U) https://tech.hindustantimes.com/government-officials-ordered-to-use-nic-email

(U) Pakistan-based hackers targeting critical infrastructure PSUs in India

(U) Pakistan-based hacker groups have expanded their cyber-attack network in India and are now targeting high-profile targets from critical infrastructure PSUs from telecom, power and finance sectors in the country, a new report warned on Friday. In October 2020, reports surfaced that Pak-based Advanced Persistent Threat (APT) groups targeted Indian defense units. The new findings from cyber security firm Seqrite have revealed that active since 2019, the APT ‘Operation SideCopy’ appears to be a cyber espionage campaign by Pakistan-backed ‘Transparent Tribe’ group that is now targeting critical infrastructure PSUs in India.
Source: (U) https://www.communicationstoday.co.in/pakistan-based-hackers-targeting-critical-infrastructure

TLP: WHITE

Sensitivity/ Handling Notice:
Sources may use **TLP: WHITE** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.