TLP WHITE
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.

AVIATION ISAC Fifth Summit
The Future of Aviation Cybersecurity: Navigating the Threat Landscape
aisac-summit.com | @AviationISAC | September 19-21, 2018 | Kissimmee, FL

www.aisac-summit.com

Aviation-ISAC Daily Aviation Memo
22 May 2018

Cyber Security News

- **Intel Warns that its New Spectre variant 4 patch will degrade performance up to 8%**
- **Mirai-variant attack launched from Mexico CVE-2018-10561 CVE-2018-10562**
- **The operations and economics of organized criminal email groups**
- **SamSam ransomware still active, targets Health Care Providers**
- **VMware Patches Fusion, Workstation Vulnerabilities★ CVE-2018-6962 CVE-2018-6963 CVE-2018-3639**
- **Dell Patches Vulnerability in Pre-installed SupportAssist Utility★**
- **FireEye Launches OAuth Attack Testing Platform**
- **Microsoft to Block Flash in Office 365**

Aviation Tech

- **Auckland Airport Uses Traffic and Passenger Flow Measurement Technology**

Legislation & Regulation News

- **FAA Moved Slower Than Usual on Engine Warning Ahead of Southwest Fatality**
- **UK Groups Issue Drone collision guidance to pilots and ATC Staff**

Physical Security News

- **Federal Law Leaves Marijuana in a No-Fly Zone**
- **Lab Monkey escapes and runs free in San Antonio Airport**

Miscellaneous News

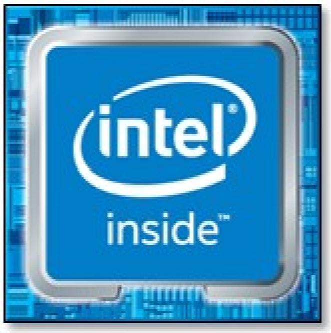
- **Saudia A330 made an emergency landing at Jeddah with the nose gear retracted**
- **Delta Creates Pop-Up Lounge for Middle Seat Passengers**

U.S. Department of Transportation Crisis Management Center Daily Report

★ *Indicates Actionable Intelligence*

FEATURES

Cyber Security News



Intel Warns that its New Spectre variant 4 patch will degrade performance up to 8%
From ZDNet (05.22.2018) Liam Tung

Intel's upcoming microcode updates to address the just-revealed Spectre variant 4 attack are likely to put a significant drain on CPU performance. Intel has anticipated questions about performance this time around by confirming upfront that its combined software and firmware microcode updates to mitigate Spectre variant 4 will cause a performance impact of up to eight percent. "If enabled, we've observed a performance impact of approximately two to eight percent based on overall scores for benchmarks like SYSmark® 2014 SE and SPEC integer rate on client and server test systems," wrote Intel executive vice president Leslie Culbertson. Spectre variant 4 is a new subclass of speculative execution attacks. Intel calls the Spectre attack a Speculative Store Bypass and calls its mitigation Speculative Store Bypass Disable (SSBD), which is delivered as a microcode update to operating system vendors, equipment manufacturers, and other ecosystem partners. Intel in January was less forthcoming in its communications about the performance impact caused by its mitigations for Spectre variant 2, only saying it would vary depending on the workload. However, Google found the impact to be significant and developed its own Retpoline software alternative. Intel's current benchmarking to test the impact of SSBD was run on unspecified Intel reference hardware and an 8th Generation Intel Core desktop microprocessor. But unlike Intel's updates for variant 2, the updates for Spectre variant 4, which is rated as a 'moderate'-severity issue and closely related to Spectre variant 1, will be optional and will by-default set to off. In this state, there is no impact on performance. In other words, if consumers and OEMs want their hardware to be extra secure they can choose that option at the expense of performance. Link

Zdnet[.]com/article/new-spectre-variant-4-our-patches-cause-up-to-8-performance-hit-warns-intel/

Mirai-variant attack launched from Mexico
From SC Media (05.21.2018) Doug Olenick

A pair of Trend Micro research teams has detected and done a quick cyber autopsy on a new Mirai-like attack that popped up in Mexico earlier this month targeting Gigabit Passive Optical Network (GPON) home routers and IP webcams. The attacks, which ran from May 8-10, sprang from 3,845 IP addresses located in Mexico and targeted routers and webcams using default passwords. Once the IoT device is entered the threat actors use CVE-2018-10561 or CVE-2018-10562 to inject malware that can enable remote code execution. Four variants of the malware are used targeted at different processor architectures ARM, ARMv7, MIPS and MIPS little-endian. Trend Micro used the Autonomous System Numbers (ASN) of the corrupted IP devices to track their location. In this case, ASN 8151 was found, which belongs to the Mexican telecom Uninet, according to Neustar's ASN lookup tool. In addition, the WHOIS data from the IP addresses also indicated they are owned by the same Mexican firm. Trend Micro's researchers reiterated the facts that attacks like this Mirai variant can be blocked or defeated through the simple expedients of changing the default login credentials and by making sure an IoT device is running the most up to date version of its software. Link

Scmagazine[.]com/mirai-variant-attack-launched-from-mexico/article/767506/

The operations and economics of organized criminal email groups
From Help Net Security (05.22.2018)

Nine of the 10 captured organized criminal email groups operate out of Nigeria, they all leverage a multitude of attack methods, and business email compromise (BEC) is far more lucrative than any other attack, according to Agari. “While much of the high-profile attention paid to email security has focused on nation state actors, the reality is that American businesses are far more likely to be attacked by BEC scammers operating from Africa,” said Patrick Peterson, executive chairman, Agari. “The sad irony is that these foreign adversaries are using our own legitimate infrastructure against us in attacks that are far more damaging and much harder to detect than any intrusion or malware.” Business email compromise leverages a variety of identity deception techniques, such as display name deception, to bamboozle organizations into making fraudulent payments. Typically, an attacker will impersonate the CEO of a company and request immediate payment to a vendor from its accounting team. In May 2018, the FBI IC3 “2017 Internet Crime Report” indicated that BEC losses increased to $675 million during 2017, more than 300 percent compared to $215 million in 2014. Researchers analyzed a variety of email based attacks, including romance scams and rental scams, but even though BEC did not emerge as a trend until 2016, BEC attacks account for 24 percent of all attacks analyzed. BEC attacks produce more victims and result in higher dollar losses than any other criminal email attack. BEC attacks are also ten times more likely to produce a victim if the target answers an initial probe email, such as “Are you at your desk to make a payment?” Link

Helpnetsecurity[.]com/2018/05/22/criminal-email-groups/

SamSam ransomware still active, targets Health Care Providers

From SC Media (05.22.2018) Doug Olenick

Allied Physicians of Michiana, Mich. reported it was hit with a SamSam ransomware attack earlier this month, but was able to quickly restore its systems and the healthcare facility does not believe any patient data was compromised. The attack took place on May 17 and company CEO Shery Roussarie said in a statement that the computer network was quickly shut down to contain the cyberattack. While Roussarie did not say how long the firm's systems were impacted, but indicated its internal IT team working with an outside incident responder and counsel was able to restore operations “without any significant disruption of services.” Allied Physicians believes the situation has been contained and it is conducting additional forensic work to confirm that personal and protected health information was not compromised during the attack. The FBI, which is also involved in the investigation, told Allied ransomware attacks are usually geared toward obtaining a financial payout and are not designed to extract information, Roussarie said. Allied did not indicate whether or not a ransom was demanded. Link

Scmagazine[.]com/allied-physicians-hit-with-samsam-ransomware/article/767654/

★ VMware Patches Fusion, Workstation Vulnerabilities

From Security Week (05.22.2018) Eduard Kovacs

VMware informed customers that updates for its Fusion and Workstation products patch important denial-of-service (DoS) and privilege escalation vulnerabilities. According to VMware, Fusion 10.x on macOS is impacted by a signature bypass flaw that can be exploited for local privilege escalation. The security hole, tracked as CVE-2018-6962, was discovered by a researcher from Chinese company Ant Financial. The issue has been fixed with the release of VMware Fusion 10.1.2.

VMware also revealed that Workstation 14.x on any platform and Fusion 10.X on macOS are impacted by several DoS vulnerabilities.   "VMware Workstation and Fusion contain multiple denial-of-service vulnerabilities that occur due to NULL pointer dereference issues in the RPC handler. Successful exploitation of these issues may allow an attacker with limited privileges on the guest machine trigger a denial-of-Service of their guest machine," the company said in its advisory. The flaw is identified as CVE-2018-6963. The issue was addressed with the release of Workstation 14.1.2 and Fusion 10.1.2. VMware on Monday also published an advisory describing the impact of a recently uncovered speculative execution attack method on its products. Researchers disclosed the details of two new issues, related to the Meltdown and Spectre attacks, that have been dubbed Variant 3a and Variant 4. VMware says Variant 4, tracked as CVE-2018-3639, affects vSphere, Workstation and Fusion. Updates for these products enable Hypervisor-Assisted Guest mitigations for this vulnerability. Link

Securityweek[.]com/vmware-patches-fusion-workstation-vulnerabilities

★ Dell Patches Vulnerability in Pre-installed SupportAssist Utility

From Security Week (05.21.2018) Ionut Arghire

Dell recently addressed a local privilege escalation (LPE) vulnerability in SupportAssist, a tool pre-installed on most of all new Dell devices running Windows. The security issue resides in a kernel driver the tool loads, Bryan Alexander, the security researcher who discovered the issue, reveals. The Dell SupportAssist tool is mainly used to troubleshoot issues and offer support to both the user and Dell. The vulnerability can be abused to bypass driver signature enforcement (DSE) ad infinitum, the researcher says. The driver, he explains, exposes a lot of functionality. The impacted driver is first loaded when SupportAssist is launched. Although used by Dell, the driver is built by PC-Doctor, a company that offers "system health solutions" to computer makers such as Dell, Intel, Yokogawa, IBM, and others. To exploit the issue, one can start reading physical memory looking for process pool tags, then identify a target process and a SYSTEM process, and then steal the token. Link

Securityweek[.]com/dell-patches-vulnerability-pre-installed-supportassist-utility

FireEye Launches OAuth Attack Testing Platform

From Security Week (05.22.2018) Ionut Arghire

FireEye on Monday announced the availability of a platform to allow organizations and pentesters check their ability to detect and respond to OAuth abuse attacks. OAuth 2.0 is a protocol employed by major Internet companies, including Amazon, Google, Facebook, and Microsoft, to facilitate granting third-party applications access to user data. Using social engineering, attackers can trick victims into authorizing a third-party application to access their account, thus gaining access to all of the user's data without the need for credentials. In an OAuth authorization flow, the third-party application requests a specific type of access to a user’s account, and APIs are used to define such sets of scopes (similar to the permissions apps ask for on mobile devices). An attacker looking to abuse OAuth can create a malicious application and then retrieve user data with the help of obtained access tokens, via the API Resource. Access tokens don’t require a password and can bypass any two-factor enforcement in place, and access to the OAuth application has to be explicitly revoked to prevent abuse. An attacker can obtain OAuth tokens via social engineering, by convincing the victim to click a “Consent link” and approve the application. This is exactly what happened last year, when a phishing attack targeting Gmail users spread like a worm and tricked many users into allowing a malicious app named “Google Docs” to access their contact information. Called **PwnAuth**, the newly launched web application framework should make it easier for organizations to test their ability to detect and respond to OAuth abuse campaigns. Available on GitHub, the platform comes with a module to support malicious Office 365 applications capable of capturing OAuth tokens and using them to interact with the Microsoft Graph API. However, PwnAuth could be used to target any cloud environment that allows OAuth applications. Link

Securityweek[.]com/fireeye-launches-oauth-attack-testing-platform

Microsoft to Block Flash in Office 365

From Bleeping Computer (05.22.2018) Catalin Cimpanu

Microsoft announced plans last week to block Flash, Shockwave, and Silverlight content from activating in Office 365. The block will only apply to Office 365 subscription clients, but not to Office 2016, Office 2013, or Office 2010 distributions, the company said. This is a full-on block, and not just Microsoft disabling problematic controls with the option to click on a button and view its content. The block means that Office 365 will prevent Flash, Shockwave, or Silverlight content from playing inside Office documents altogether. The change is set to come into effect starting with January 2019. Only Flash, Shockwave, and Silverlight content embedded with the "Insert Object" feature are blocked, but not those embedded via "Insert Online Video." The difference is that the former uses Microsoft's OLE (Object Linking and Embedding) technology, while the latter embed content via an Internet Explorer browser frame. Microsoft cited different reasons for taking this decision. It said that malware authors have abused this mechanism for exploit campaigns, but also that Office users rarely used these features anyway. In addition, Microsoft said it was also taking this decision after Adobe announced Flash's end-of-life for 2020. In case some companies still need to embed or view Flash or Silverlight-based content in Office 365, Microsoft has published a support page with guidance on how to re-enable Flash, Silverlight, and Shockwave controls. Link

Bleepingcomputer[.]com/news/microsoft/microsoft-to-block-flash-in-office-365/

Aviation Tech

Auckland Airport Uses Traffic and Passenger Flow Measurement Technology

From Airport Technology (05.21.2018)

Growing passenger numbers are impacting airports worldwide, including Auckland International Airport in New Zealand, which handled 19 million passengers in 2018. The airport is taking the increased passenger flow and logistics issues seriously, using a unique combination of traffic and passenger flow measurement technology. To cope with an increase in passenger load, the airport embarked on a wide-ranging and world first combined passenger-flow and road-traffic measurement project, with the goal of obtaining a real-time cohesive view of people movement patterns, to guide daily and long-term operational decisions, maximize capacity and improve flow. With several traffic monitoring projects in New Zealand, using the same technology, infrastructure consultants Beca was commissioned to extend the solution across the airport’s roading infrastructure. This now provides the airport with a seamless picture of traffic flow information between the airport and Auckland CBD (Central Business District, also called the city center). Outside the airport, the solution measures traffic flow between the CBD and the airport, providing real-time data on reliability, vehicle counts and travel time. The insights, collected using a range of technologies, including radar and Wi-Fi sensors, also helps the New Zealand Traffic Agency (NZTA) to make informed traffic management decisions, and has allowed for the implementation of a number of initiatives to improve the traffic flow to the airport. In addition, the real-time and historic BlipTrack data enables NZTA, via their new app RideMate and online, to display live travel times between the CBD and airport, as well as informing about days with a high risk of congestion. Inside the airport, the solution provides metrics on passenger queue times and volume, as well as insight into passenger movement patterns throughout the international and domestic terminals´ departure and arrival processes. Link

airport-technology[.]com/contractors/asset_management/veovo/

Legislation & Regulation News

FAA Moved Slower Than Usual on Engine Warning Ahead of Southwest Fatality

From The Wall Street Journal (05.20.2018) Andy Pasztor

Investigators have yet to issue their final report on a Southwest Airlines Co. flight last month that ended in an emergency landing and a passenger's death. But one thing is clear: Despite a warning about a suspect engine part nearly two years earlier, investigators didn't mandate enhanced inspections for an unusually long time and acted only after the high-profile fatality. Questions about the time it took regulators to mandate more comprehensive inspections—and whether an alternate response would have made a difference in uncovering what emerged as the greatest danger—remain unanswered. More than any commercial aviation accident in recent years, circumstances surrounding last month's events have spurred industry officials, regulators and independent experts to reassess the best way to identify, rank and combat risks in an industry where safety statistics have become so exemplary. In the April accident, serious metal fatigue caused a single, fast-moving engine-fan blade to break into pieces at roughly 32,000 feet. The violent rupture ended up spewing remnants of the front engine cover into the plane's wing and body, killing a passenger who was partly sucked out a window that had been destroyed by the debris. A similar but nonfatal accident in August 2016 drew industry attention to the potential for blades in the engines to crack, after the engine maker quickly notified regulators and some airlines that it was working on stepped-up inspection procedures. Roughly seven months later, the engine maker began recommending ultrasound inspections, rather than just visual checks, for certain fan blades based on the number of flights in service. Several months after the manufacturer's initial recommendation, the Federal Aviation Administration proposed similar stepped-up checks. But the FAA was still weeks away from making those checks mandatory when last month's fatal accident occurred. After that, some airlines accelerated voluntary inspections almost immediately, and the FAA quickly mandated comprehensive inspections, which are now under way.Link

Wsj[.]com/articles/faa-moved-slower-than-usual-on-engine-warning-ahead-of-southwest-fatality-1526814000

UK Groups Issue Drone collision guidance to pilots and ATC Staff

From Air Traffic Management (05.22.2018)

British pilot and air traffic control bodies have worked together to create guidance in preventing drone collisions. The British Airline Pilots' Association (BALPA) and the Guild of Air Traffic Control Officers (GATCO) have created the guidelines due to concerns over a lack of national guidance. Drone sightings by commercial aircraft are on the rise, going from zero reports in 2013, steadily rising over the last few years, with 2017 seeing 92 reports in UK airspace – something likely to rise further once the Airprox analysis has been completed The UK and many other countries do not yet have standard procedures to deal with drone sightings near aerodromes or violations of controlled airspace by drones. Both organizations have issued the guidance to their members in an effort to give pilots and air traffic controllers steps to follow should a drone be flown in an irresponsible manner that puts other airspace uses in danger. They advise that when a drone report is received, pilots should reduce speed to minimum clean during climb and descent, and reduce speed to 180kt during approach. They recommend that the speed reduction should be requested first so ATC can assess the traffic situation and accommodate the request safely. Further speed reductions below 180kt can be requested but may not be possible due to final approach separation requirements. If a drone is seen, pilots must report the sighting to ATC and provide as much accurate information as possible. It is particularly important to pass sufficient information to ATC to positively identify it as a drone so the report should contain: its location; altitude; lateral and vertical separation; whether it was moving or stationary as well as its size, shape and appearance. Link

Airtrafficmanagement[.]net/2018/05/drone-collision-guidance-issued-to-pilots-and-air-traffic-control/

Physical Security News

Federal Law Leaves Marijuana in a No-Fly Zone

From City Lab (05.21.2018) Leslie Nemo

There's still a lot of confusion around legal marijuana. Though banned federally, each state, and even county, decides what kind of marijuana is allowed, and users don't always know what those lines are. One of the spaces that catches people by surprise? Airports. Commercial flights work under federal law, and boarding them requires passing inspection by the Transportation Security Administration (TSA), another federal operation. Because airports are the boundary between local and national rule, staff and security have to negotiate the transition with pot-carrying passengers leaving marijuana -legal towns. For some, the solution has been amnesty boxes. These bright-green mini mailboxes at airports let passengers anonymously deposit marijuana or any illegal substances. The contents are regularly emptied by police or private contractors and destroyed. As a last-minute opportunity to dodge a felony, the boxes have probably saved some people from citations, fines, and jail time, but they do the airports some favors, too. When Colorado Springs Airport put in amnesty boxes in 2014, they were tired of marijuana being trashed, flushed, and buried on their property, said Aidan Ryan, the airport's marketing and communications manager. Marijuana had been legalized in the state two years earlier, and marijuana tourists were showing up to the airport and finding out that it's a federal crime to carry their purchases onto planes, even if the flight departs from and arrives in marijuana -legal places. Also, TSA must report any amount or derivative of marijuana to airport security if they see it during screening. To alert passengers and facilitate compliance with the law, the airport became the first to install the lime green boxes. The bins work like mailboxes: Once something goes in, it can't come out. Colorado Springs Airport Police empty the boxes once a month, and they almost always have something in them, Ryan says**.** Link

Citylab[.]com/life/2018/05/federal-law-leaves-marijuana-in-a-no-fly-zone/560663/

Lab Monkey escapes and runs free in San Antonio Airport

From The Independent (05.22.2018) Jane Dalton

A monkey once used in medical experiments has been caught and taken to a sanctuary after a daring bid for freedom at one of America's biggest airports. Dawkins, a rhesus macaque, managed to escape from his transport crate at San

Antonio International Airport, and evaded capture for up to an hour. The animal, said to be stressed and frightened, was being transported to the Born Free USA wildlife sanctuary in La Salle County, Texas, where conservationists want him to adjust to living outdoors. He escaped after arriving on an American Airlines flight from Chicago, while the cargo was being offloaded, and wandered around the cargo bay. The airport's wildlife biologist worked with vets and staff from the San Antonio Zoo to corner him in a baggage-handling area before giving him a tranquillizer dart, said Russ Handy, San Antonio's aviation chief. Link

Independent[.]co[.]uk/news/world/americas/monkey-lab-tests-texas-airport-escape-san-antonio-born-free-a8362966[.]html

Miscellaneous News

Saudia A330 made an emergency landing at Jeddah with the nose gear retracted

From News in Flight (05.22.2018)

A Saudia Airbus A330 made an emergency landing with its nose gear retracted at Jeddah's King Abdul Aziz International airport on 21 May 2018. The A330 flight #SV3818 from Madinah, Saudi Arabia to Dhaka, Bangladesh, with 141 passengers and 10 crew members on board circled about 3,5 hours before making an emergency landing. Saudi Arabia's Aviation Investigation Bureau said, decision was made to divert to Jeddah after a defect in aircraft's hydraulic system which caused the nose gear to stay retracted. The aircraft landed without its nose landing gear deployed and came to a stop on its front belly, supported by its main landing gears. Passengers were safely evacuated using emergency slides. No injuries were reported Link

Newsinflight[.]com/2018/05/22/saudia-a330-flight-sv3818-made-an-emergency-landing-at-jeddah-with-the-nose-gear-retracted/

Delta Creates Pop-Up Lounge for Middle Seat Passengers

From Airline Geeks (05.22.2018) Akhil Dewan

Oftentimes, passengers who are stuck with the middle seat on an airplane are considered the unlucky ones. From battling over armrests, missing out on the views of the ground below, and being squished between to random strangers, the benefits of a middle seat are slim to none. However, middle seat passengers flying out of Boston Logan International on Delta yesterday were offered a unique perk. Atlanta-based Delta Air Lines teamed up with Atlanta-based Coca-Cola to offer the Middle Seat Lounge. Passengers can enjoy VIP treatment by receiving free Coca-Cola along with other middle seat-ers, playing games, meeting former NBA champion and Boston Celtic, Brian Scalabrine, and receiving specially branded Coca-Cola bottles to share with their seatmates. Additionally, passengers can even win a free trip with the airline by posting a selfie with their seatmates on board the aircraft. This isn't the first time the two companies have partnered up to offer passengers a unique flying experience. In 2017, Delta and Coca-Cola created an art contest to transform tray tables on board a Boeing 767 into works of art inspired by the some of the airline's destinations, including Amsterdam, Atlanta, London, Mexico City, and Shanghai. Link

Airlinegeeks[.]com/2018/05/22/delta-creates-pop-up-lounge-for-middle-seat-passengers/

U.S. Department of Transportation Crisis Management Center Daily Report
Commercial In-Flight Incidents

- **UPS 63, B748**
  - May 21, 2018 at 8:15 PM EDT
  - Enroute from Anchorage, AK (Ted Stevens Anchorage International Airport) to Louisville, KY (Louisville International Airport)
  - Hit runway approach lights on departure
  - Returned to Anchorage, AK; landed without incident at 9:22 PM EDT
- **UPS 4985, B763**
  - May 21, 2018 at 7:26 PM EDT
  - Enroute from Seattle, WA (Boeing Field) to Louisville, KY (Louisville International Airport)
  - Electrical system problem
  - Diverted to Spokane, WA (Spokane International Airport); landed without incident
- **Southwest 1674, B737**
  - May 21, 2018 at 12:22 PM EDT
  - Enroute from Austin, TX (Austin–Bergstrom International Airport) to Denver, CO (Denver International Airport)
  - Oil pressure problem
  - Returned to Austin, TX; landed without incident
- **United 1148, B772**
  - May 21, 2018 at 10:26 AM EDT

  - Enroute from Newark, NJ (Newark Liberty International Airport) to Los Angeles, CA (Los Angeles International Airport)
  - Flight control problem
  - Returned to Newark, NJ; landed without incident at 10:46 AM EDT

Ground Incidents

- **Newark, NJ, Newark Liberty International Airport**
  - May 22, 2018 at 3:14 AM EDT
  - United 2160, B752, scheduled from San Francisco, CA (San Francisco International Airport)
  - Smoke from engine; hydraulic fluid leak
  - Passengers deplaned via stairs; bussed to terminal
  - No impact to operations
  - 0 fatalities; 0 injuries

The Daily Aviation Memo is a daily update of foreign and domestic commercial aviation news compiled from open sources and commercially-available information. Information contained in this report is provided for situational awareness only and does not represent the views of the Aviation ISAC. Please send comments or distribution requests to a-isac.advisory@a-isac[.]com.

A-ISAC Intel Shop
Dblough@a-isac.com
Ralvillar@a-isac.com
phart@a-isac.com
rforczyk@a-isac.com
a-isac.ops@a-isac.com
Aviation Information Sharing and Analysis Center (A-ISAC)
AVIATION ISAC
www.a-isac.com