



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

CONNECT to PROTECT

INFORMATION TECHNOLOGY SECTOR

27 January 2022

LIR 220127006

Foreign Adversaries' Use of Cloud Storage to Access, Transfer, and Store Sensitive Data

References in this LIR to any specific commercial product, process, or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service, or corporation on behalf of the FBI.

This Liaison Information Report (LIR) uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, Version 8. See the [ATT&CK for Enterprise framework](#) for referenced threat actor techniques and for mitigations.

The FBI Indianapolis Field Office, Los Angeles Field Office, and Counterintelligence Division, in coordination with Office of Private Sector (OPS), prepared this Liaison Information Report (LIR) to inform private sector partners about foreign adversaries' use of cloud storage^a platforms to access, transfer, and store sensitive or proprietary information quickly and without detection. Foreign adversaries have adapted new ways to covertly acquire and transmit sensitive or proprietary information utilizing cloud storage platforms, thus enabling them to further gain unfair competitive advantages against U.S. corporations and research institutions.

Utilizing Cloud Storage Platforms to Access and Transfer Sensitive Data

With U.S. companies increasingly embracing digital solutions, unauthorized access to private computer networks by witting or unwitting actors could potentially expose sensitive information to foreign adversaries. This includes cloud storage services [[T1567.002](#)] operated by both U.S. and foreign corporations. Most major cloud service applications provide users the ability to remotely store specific files from their devices and secure them with usernames and passwords. Those that offer "zero knowledge," or private, end-to-end encryption (E2EE),^b allow users to encrypt data prior to its storage on the cloud, ensuring the services are unable to view the data in its raw, unencrypted format. Encrypted communications applications can also be used to move materials to a cloud server.

- In April-May 2020, a lawful permanent resident (LPR) associated with a foreign talents program downloaded over 100,000 documents from his/her U.S. employer's network, which he/she copied to an external storage device [[T1052.001](#)]. The LPR used several different U.S. and foreign-based cloud storage and file sharing applications to collaborate with others, including other foreign nationals tied to talents programs.

^a For the purposes of this LIR, cloud storage is defined as a service model in which data is transmitted and stored on remote storage systems, where it is maintained, managed, backed up, and made available to users over the Internet. Cloud-based data is stored in logical pools across disparate, commodity storage servers located on premises or in a data center managed by a third-party cloud provider. Cloud service providers manage and maintain data transferred to the cloud, eliminating the need for organizations to buy, manage, and maintain in-house storage infrastructure (from article <https://searchstorage.techtarget.com/definition/cloud-storage>.)

^b The FBI remains concerned that the use of E2EE communications and messaging applications by foreign adversaries and other threat actors continues to impede FBI and domestic law enforcement investigations, resulting in the loss of irreplaceable electronic evidence and investigative leads, even when a judicial order has been issued allowing lawful access to a subject's data and communications.



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

CONNECT to PROTECT

- In late September 2018, a federal grand jury indicted Chinese state-owned enterprise Fujian Jinhua Integrated Circuit, Co., Ltd., Taiwan-based United Microelectronics Corporation (United), and three individuals for conspiracy to steal a U.S. semiconductor company's trade secrets and convey them to a company controlled by the Chinese Government. Under a cooperative agreement, Fujian Jinhua would mass produce transferred technology for United. Before leaving the U.S.-based company, one of the individuals allegedly downloaded more than 900 confidential and proprietary files to external hard drives or cloud storage, from which he/she could access them while working at Fujian.
- In November 2017, a foreign national uploaded sensitive files to a Chinese-based cloud service account he/she created several months before accepting employment at a U.S.-based electronics equipment designer and manufacturer. The foreign national claimed to use the account to store photos, videos, family information, and work files from a previous employer and as a computer backup.

Mitigation and Best Practices

U.S. private sector partners should maintain robust security protocols for access to their research and proprietary information, particularly with increased work from home and the use of cloud platforms to house sensitive data. This includes understanding the risks associated with foreign entities' potential access to sensitive data or computer networks, as well as cloud service providers that utilize servers located abroad. In some cases, foreign entities could be forced to surrender data to foreign governments, in compliance with other countries' laws or regulations (see FBI PIN 20200624-001 titled "[Risks of Using Foreign Unmanned Aircraft Systems during COVID-19 Pandemic](#)" dated 24 June 2020).

Companies and research institutions should carefully monitor the use of cloud storage platforms on work systems. The FBI has identified the following best practices, which may assist private sector partners protect their sensitive data and intellectual property:

- Educate and regularly train employees, contractors, visitors, and consultants on security policies and protocols
- Train employees on research ethics so they have a clear idea of what is and is not acceptable to share outside of their lab or facilities
- Thoroughly research domestic and foreign individuals and entities when engaging in joint ventures, shared research efforts, investment opportunities, or mergers and acquisitions
- Ensure joint ventures protect your intellectual property and establish clear and enforceable penalties for violations
- Monitor computer networks routinely for suspicious activity
- Ensure proprietary and pre-publication information is carefully protected and monitored
- Engage with federal, state, and local law enforcement for threat awareness and risk management
- Restrict Web-Based Content [[M1021](#)] – Web proxies can be used to enforce an external network communication policy that prevents use of unauthorized external services



- Disable or Remove Feature or Program [M1042] – Disable Autorun if it is unnecessary and disallow or restrict removable media at an organizational policy level if they are not required for business operations
- Limit Hardware Installation [M1034] – Limit the use of USB devices and removable media within a network
- Apply scrutiny to which cloud storage platforms are authorized for use, accounting for applicable data retention and privacy laws as well as the platform’s risk exposure and necessity to the organization
- Maintain awareness of which cloud storage platforms have end-to-end or zero knowledge encryption

For additional information and resources, this LIR may be read in conjunction with the following products:





- FBI Slicksheet S-191212-004, “[Cloud Risks and Concerns Across Industries](#),” dated 12 December 2019
- National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and FBI joint Cybersecurity Advisory, “[Russian SVR Targets U.S. and Allied Networks](#),” dated 15 April 2021
- FBI, DHS, and CISA Joint Cybersecurity Advisory, “[Russian Foreign Intelligence Service \(SVR\) Cyber Operations: Trends and Best Practices for Network Defenders](#),” dated 26 April 2021
- United Kingdom National Cyber Security Centre, CISA, FBI, and NSA joint Alert, “[Further TTPs associated with SVR cyber actors](#),” dated 07 May 2021

To report suspicious activity or other incidents involving intellectual property, please visit the Internet Crimes Complaints Center at www.ic3.gov and/or the National Intellectual Property Rights Coordination Center at www.iprcenter.gov. If you believe your company’s intellectual property has been targeted or is at risk of compromise, please contact your local FBI Field Office.

The OPS Information Sharing and Analysis Unit disseminated this LIR. Direct any requests and questions to the Private Sector Coordinator at your local FBI Field Office:
<https://www.fbi.gov/contact-us/field-offices>.



Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	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.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.