SECURE TOMORROW SERIES

SCENARIO NARRATIVE 1: LIFE UNDER A MICROSCOPE

The Cybersecurity and Infrastructure Security Agency (CISA) has produced these scenarios to initiate and facilitate discussion. The situations described here are hypothetical and speculative and should not be considered the position of the U.S. government. All names, characters, organizations, and incidents portrayed in these scenarios are fictitious.

ON "CYBER AND PHYSICAL ATTACKS ON ATOMICA NUCLEAR POWER PLANT PERSONNEL"

A HEARING BEFORE THE SENATE HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS COMMITTEE AND U.S. SENATE COMMITTEE ON ENERGY AND NATURAL RESOURCES WRITTEN TESTIMONY SUBMITTED BY FBI CYBER DIVISION DIRECTOR JONATHAN STYLE

September 18, 2026

Chairman, Chairwoman, Ranking Members, and members of the Committees, thank you for the opportunity to testify before you today regarding the Federal Bureau of Investigation's (FBI) and our federal partners' efforts to understand, mitigate, and respond to the recent cyber and physical attacks on personnel from the Atomica nuclear power plant. We take these recent attacks with the utmost seriousness. The initial response of the U.S. government was swift and measured; however, we must do more to ensure that critical infrastructure operators are protected and that we are not vulnerable to such attacks in the future. Part of doing more is understanding the history and environment that has led to such attacks, while also assessing and mitigating against future risks.

INCIDENT ASSESSMENT

Between November 2025 and May 2026, a series of cyber and physical attacks, some successful, were executed against a number of security and key operational personnel from the Atomica nuclear power plant. The attacks were highly targeted to those individuals, as demonstrated by the fact that the attackers had privileged, private, and sensitive information on the individuals' identities, locations, and personal habits.

Since the first attacks, FBI, other components of the Department of Justice (DOJ), and the Department of Homeland Security Cybersecurity and Infrastructure Security Agency have worked closely to attribute and mitigate the source of these attacks. The FBI's Cyber Division is responsible for investigating, dismantling, and prosecuting cybercrimes. Through our efforts, many of the perpetrators have been identified, pursued, and arrested.

Initially, we faced challenges in our ability to identify the sources of personal and sensitive information that enabled these attacks. It was not until June 12, 2026, when information obtained by a major news outlet provided us with the break that we were searching for. The media source implicated a third-party data broker, SecurePI, in the sale of sensitive data on Atomica personnel to a

foreign corporation with close ties to Russia. For those unaware, SecurePI has been helping Atomica revamp its personnel security and has been assisting the company in managing the sensitive information collected during security and background investigations.

We have been able to attribute the breach of sensitive data to an insider who worked at SecurePI. This individual had access to the information necessary to review and grant access control and security privileges. The individual responsible for the breach was paid to produce analytical products for Russia to allow micro-targeting of individuals. The data sold also included packets of data that were de-anonymized to allow Russia to amass a great deal of information on these individuals and their families.

DOJ and our partner agencies have taken swift action against that individual and against the Russian government.

FACTORS CONTRIBUTING TO THE ATTACKS

Although an insider clearly enabled these attacks, other factors, many dating back more than a decade, have contributed to the ability of this type of breach to occur. The prevalence of third-party data brokers is one such contributing factor.

Third-party data brokers generate, for profit, consumer profiles by piecing together information from a variety of disparate and unrelated sources. It is now faster and cheaper, not to mention more thorough, to conduct a search with one of these brokers than to go through almost any public sector process. By 2023, standard practice was to engage data brokers to run background checks on people rather than to use police departments. The popularity of these data brokers has skyrocketed, and they are used regularly around the country for job applicants, prospective tenants, childcare workers, identity verification, and loans.

Make no mistake, these companies collect potentially sensitive information about individuals such as financial fitness, employment history, political affiliations, webpages frequently visited, close social connections, and categorization into social groups for all manner of applications. Our society has become increasingly reliant on these companies in order to function. Today, local, state, and federal government agencies in the U.S. are developing processes to integrate a pseudo social-credit system—leveraging a variety of social and civic behavioral indicators along with financial indicators—through the use of third-party data brokers. Local law enforcement departments nationwide are using these systems to support investigations, which have enhanced safety and policing and improved public relations. For security reasons, the U.S. government has limited its use of third-party data brokers to those that are owned and operated in the U.S. Ironically, the adoption of third-party data brokers was driven at least in part to help address insider threats and help organizations better assess job applicants and monitor employees. Unfortunately, as we have seen, these services are not without their own risks.

Another contributing factor is simply the amount of data that third-party data brokers (and other organizations) have on individuals, including critical infrastructure owners and operators. The largest data brokers have amassed thousands of data points on billions of individuals worldwide. The individuals who executed the attacks leveraged personal information on Atomica personnel, including location-tracking data and personal habits, to target their cyber and physical activities. Over the past decade, the proliferation and collection of this type of personal data corresponded to the proliferation of connected personal digital/virtual assistants (often referred to as Internet of Things (IoT) devices), along with a decrease in society's concern about online and personal privacy.

Many credit these changes in connectedness and the decrease in privacy to a post–SARS-19 world. As the U.S. (and the world) recovered from SARS-19 and rebounded from the concurrent economic impacts, concerns about online privacy seemed to dwindle. In the late 2010s, we saw increasing concern over individuals' cybersecurity and privacy, as exemplified by the European Union's General Data Protection Regulation (GDPR) legislation. But by 2023, the tides seemed to have turned. Little privacy legislation was enacted in the post–SARS-19 period. There was also little public dissent to online tracking, as the benefits of enabled devices seemed to outweigh any hypothetical costs. Without privacy legislation, the rise in IoT-enabled and connected devices corresponded with a decrease in real-world privacy. Individuals these days expect little privacy when their real-world movements and online activities are continuously tracked.

Before proceeding, I would like to note that my intention today is not to make a case against IoT-enabled devices but, rather, to highlight the complex nature of enabling digital connectivity while maintaining privacy and security. In the post–SARS-19 era, IoT devices, coupled with rapid data transmission enabled by 5G networks, have been employed with great benefit to the U.S. and other nations. For example:

- Health-status tracking apps (deployed on personal devices) enabled the rapid collection and dissemination of contact tracing and SARS-19 vaccination and immunity data tracking. Despite initial resistance, pandemic fatigue and the desire for a "return to normal" made the majority of those in the U.S. eventually assent to this collection and dissemination of data.
- The SARS-19 pandemic also led to an increase in remote work, which many employees and companies sought to continue, at least in part, after the pandemic. As more employees and companies turned to telework and as more people grew accustomed to a virtual world, the market for IoT-enabled devices that would help them work at home (e.g., mixed reality and augmented reality devices, automated system monitoring and control devices, predictive maintenance devices) boomed.
- The SARS-19 pandemic also demonstrated weaknesses in the U.S. supply chain for some critical supplies and resources (e.g., food, paper products, and medical supplies). In addition to increasing U.S. manufacturing capabilities in these areas to secure the supply chain, real-time IoT- and 5G-enabled tracking gave suppliers a much clearer picture and control of critical supplies, including the ability to rapidly assess and reroute shipments to areas of need.
- Beginning in 2020, deployment of 5G increased internet access to many rural areas, achieving more than 70 percent penetration in the U.S. by the end of 2025.

As these benefits were realized, the proliferation of IoT and advanced wireless technologies continued, leading to parallel growth in data collected on individuals and an increase in sensitive data collected and stored by organizations.

FUTURE THREAT ASSESSMENT

Looking forward, the risks—both cyber and physical—presented by the proliferation of sensitive data collection and the limitations of privacy protections will persist. Additional factors exist that can contribute to the feasibility and criticality of cyber and physical attacks on organizations and individuals. Specifically, a lack of security standards for cloud infrastructure and IoT devices presents considerable challenges to securing cyberspace, a topic on which I have testified previously.

To provide you with a bit of background, an increasing number of companies started taking advantage of cloud services, continuing a trend that began prior to the 2020s, especially as the amount of data these companies needed to store increased and the cost of cloud services

decreased. Since 2020, the amount of sensitive data stored in the cloud has increased exponentially. Additionally, cloud users can access a variety of cloud services, including both cloud and hybrid architectures. However, as organizations began to implement multi-cloud infrastructures, many lacked—and continue to lack—a thorough understanding of their entire cloud footprint. Many do not appreciate that cloud security is a shared responsibility between the provider and users. A lack of cloud IT security professionals also contributes to the number of poorly secured cloud infrastructures.

Meanwhile, IoT devices often lack appropriate security. Some attempts have been made to secure IoT infrastructure, such as the 2020 IoT Cybersecurity Improvement Act. Unfortunately, that act and others that followed have done little to improve the nation's overall IoT security because they failed to sway a sufficient number of manufacturers into adopting the prescribed standards. Although market forces have encouraged IoT device security, the rapid expansion in the number of IoT devices and the lack of security requirements still resulted in many poorly secured networked devices.

Poorly secured cloud infrastructures and IoT devices present a multitude of easy access points for sensitive data and systems. Although this attack on Atomica personnel was the result of an insider threat, in the current environment an insider is not required to gain access to sensitive data in many cases. To help manage and attempt to secure sensitive and personal data, many organizations are leveraging data Security as a Service (SECaaS) and Disaster Recovery as a Service (DRaaS); however, this is not enough. The rapid expansion of IoT devices, rapid data transmission rates, instances of insecure IoT devices and cloud services, and the data available on individuals and organizations put the U.S. in a vulnerable position. This vulnerability is exemplified by the fact that over the past few years there has been a dramatic increase (500 percent since 2022) in the number of successful cyberattacks.

With rapid data transmission rates, nefarious actors are able to exfiltrate massive amounts of data in a very short amount of time. They need only very brief access to a system to steal terabytes and even petabytes of data, making automatic network defenses less effective. The rollout of many insecure IoT devices in the critical manufacturing sector has led to vulnerabilities from industrial espionage in critical supply chains. Unfortunately, the ability to move large amounts of data rapidly and the rapid expansion of cloud users and services has also made movement of data, and thus data provenance, harder to track.

Understanding and identifying these risks is not the principal challenge we face. Rather, our principal challenge is determining how we can reverse course in some areas and take actions that support and provide the benefits of our connected world, but provide protections for sensitive personal, private sector, and government data. To counter the threats we face, the U.S. government must collaborate with the private sector to secure IoT devices, secure personal information, secure cloud infrastructures, and monitor insider threats better.

Thank you for the opportunity to appear before the Committees today, and I look forward to your questions.