

TIR-20260930 FBI Cyber Strategy 2026: What Businesses and Security Leaders Need to Know

9/30/2026

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

COPYRIGHT: Copyright © Aspire Technology Partners. All rights reserved.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

Executive Summary	3
Why the FBI Issued a Public Cyber Strategy	4
The Four Pillars	4
Disrupt Adversaries and Impose Costs	4
Support Victims	5
Strengthen Partnerships	5
Build FBI Cyber Capabilities	5
What the Strategy Means for Businesses and Security Leaders	5
ShinyHunters and the FBIJobs.gov Investigation	6
Conclusion	9
Aspire Protects	9
Supporting Documentation	10
Appendix II: Disclaimer	11

Executive Summary

The FBI is putting more emphasis on stopping cyberattacks before the damage spreads. Its 2026 Cyber Strategy, published September 9, calls for earlier victim notifications and closer coordination with private companies and foreign law enforcement.

The strategy has four pillars:

- Stop cybercriminals and make it harder for them to continue operating.
- Support victims
- Strengthen partnerships
- Build the FBI's cyber capabilities

The FBI wants to contact victims sooner when it finds evidence of a compromise. That could include a business, government agency, school, hospital, or critical infrastructure operator. Earlier notification gives the impacted organization more time to stop the attack and limit the damage. The strategy also calls for faster sharing of technical information with the security teams handling the response.

ShinyHunters became an early test for the strategy. On September 22, the group claimed it breached FBIJobs.gov and stole information belonging to FBI employees and job applicants. The FBI confirmed that it was investigating but has not established where the access began. Oracle has not confirmed the new PeopleSoft zero-day claimed by the group.

Dutch police announced on September 29 that they had arrested a suspected ShinyHunters member two weeks earlier. The FBI described the arrest as an example of

TIR SUMMARY



ASPIRE

TLDR;

- The FBI published its first cyber strategy for the year 2026.
- The FBI wants to warn U.S. organizations earlier when it finds evidence of a compromise.
- The strategy focuses on businesses, government agencies, and critical infrastructure.
- Foreign law enforcement may lead when a suspect or server is outside the United States.
- Cybersecurity firms may be asked to provide logs or technical findings.
- Businesses remain responsible for containing the attack and restoring operations.
- ShinyHunters provides an early example, but key FBIJobs.gov claims remain unconfirmed.
- Organizations should establish an FBI contact and make sure useful logs are available.

working through the partner with the legal authority to act. The arrest occurred before the FBIJobs.gov claim became public, and no evidence released so far connects the two cases.

WHY THE FBI ISSUED A PUBLIC CYBER STRATEGY

A cyberattack against a U.S. organization can be launched from anywhere in the world. Foreign governments may be after sensitive information or long-term access to critical systems. Criminal groups are usually looking for money and often use trusted vendors or shared services to reach more than one victim.

Most large cyber operations are not run by one person. Ransomware crews buy access, rent servers, and rely on other criminals to move stolen money. Taking down one member may slow the group, but it rarely ends the operation.

The FBI's strategy calls for pressure on the entire operation, including the infrastructure and funding that keep it running.

THE FOUR PILLARS

The strategy divides the FBI's cyber mission into four pillars. They explain where the bureau will focus its efforts and how that work will be carried out.

Disrupt Adversaries and Impose Costs

The FBI is not relying on arrests alone. It may also take down criminal infrastructure, recover stolen cryptocurrency, or work through another country when a suspect is beyond its reach.

The bureau calls this the "best athlete" model. The partner in the best position to act takes the lead. That may be the FBI, foreign police, another federal agency, or a company that controls an account or server used in the attack.

Support Victims

The FBI wants to warn victims before an investigation is finished. If agents find signs of a compromise, they plan to share that information while the organization can still contain the activity and preserve evidence.

Information from the victim can also move the investigation forward. A log entry or compromised account may connect the attack to other victims or infrastructure already under investigation.

Strengthen Partnerships

Evidence in a cyber case is rarely held in one place. A cloud provider may have account logs that the victim cannot see. Foreign police may have authority over a server or suspect outside the United States.

The strategy gives those partners a larger role. Private companies may be asked to provide technical information or take action against infrastructure they control.

Build FBI Cyber Capabilities

The FBI plans to hire more people with technical experience and expand the teams available during major cyber incidents. Its field offices will also have coordinators who work with organizations that operate industrial control systems.

AI tools may be used to examine malware, trace attacker infrastructure, and review large amounts of case data. The FBI says people will remain responsible for reviewing the results and making decisions. The strategy does not explain how the bureau will measure the accuracy or effectiveness of these systems.

WHAT THE STRATEGY MEANS FOR BUSINESSES AND SECURITY LEADERS

The strategy calls for the FBI to contact U.S. organizations sooner when it finds evidence of a compromise. That warning may come from information found during another investigation, before the affected organization knows there is a problem.

Private companies may also hold evidence the FBI needs. Cloud providers, software companies, cybersecurity firms, and managed service providers may have records or control infrastructure that cannot be accessed from the affected organization's network. The FBIJobs.gov investigation offers a current example. The bureau is working with companies that support the portal while it determines where the access began.

- **Cybersecurity leaders** - Security leaders should establish a verified FBI contact and decide who can act on information received from law enforcement. They also need access to the logs and systems required to check the warning.
- **Cybersecurity firms** - Managed security providers and incident response firms may be asked to provide logs or technical findings connected to an investigation. Providers should have a process for responding to those requests without exposing information belonging to unrelated customers.
- **Businesses** - FBI involvement does not transfer responsibility for the response. The affected organization must still contain the activity, restore systems, and meet any legal or regulatory requirements.
- **Business leaders and decision makers** - Leadership should decide who can authorize the release of company records and when legal counsel should become involved. They may also need to approve containment measures that temporarily interrupt business operations.
- **Critical infrastructure operators** - Organizations responsible for essential services will remain a priority because an attack could affect public safety or interrupt operations. An early warning will only help if it reaches someone who can act on it immediately.

SHINYHUNTERS AND THE FBIJOBS.GOV INVESTIGATION

The ShinyHunters case emerged less than two weeks after the FBI published its strategy. It involves a reported breach of the bureau's recruitment portal and a separate arrest in the Netherlands. Both developments involve ShinyHunters, but public information does not connect the arrest to the FBIJobs.gov case.

On September 22, ShinyHunters claimed it used a new Oracle PeopleSoft zero-day against FBIJobs.gov. No CVE has been assigned, and the reported access method remains unconfirmed.

A separate PeopleSoft vulnerability, CVE-2026-35273, was already being exploited by the group but has not been linked to FBIJobs.gov. Aspire's CTI team previously covered the vulnerability in an [Emergency Flash Notice](#). The CTI team also reported on the [Canvas and PeopleSoft security incidents](#) linked to ShinyHunters in July 2026.

The group claimed it reached other FBI services and entered an FBI-managed AWS GovCloud environment. It also said it stole two to three terabytes of information belonging to employees and job applicants.

The FBI confirmed that it was investigating unauthorized activity affecting FBIJobs.gov. The point of access remains undetermined and could involve either the FBI's environment or a company supporting the portal.

News organizations reviewed an image showing a ShinyHunters message on FBIJobs.gov before the portal was taken offline. The image supports reports that the site was defaced, but it does not show how access was gained or how much information was taken.

The Dutch arrest was announced after the FBIJobs.gov claim, but it occurred one week earlier. Without evidence connecting the two cases, the arrest should be treated as a separate ShinyHunters investigation.

TTPs (FBIJOBS.GOV CASE)

Few technical details have been released about the FBIJobs.gov case. The TTPs below are based on ShinyHunters' claims and reporting on the portal defacement, not on confirmed forensic findings.

- **Initial Access, Exploit Public-Facing Application [T1190]** - ShinyHunters claimed it used an unpatched Oracle PeopleSoft vulnerability to access FBIJobs.gov. Neither the FBI nor Oracle has confirmed that access method.

- **Collection, Data from Information Repositories [T1213]** - The group claimed it accessed personnel, applicant, and medical records. The FBI has not confirmed what information was accessed or how much data was taken.
- **Impact, Defacement [T1491.002]** - News organizations reviewed an image showing a ShinyHunters message on the FBIJobs.gov portal before it was taken offline. The FBI has not released the technical cause of the reported defacement.

THE FBI'S PUBLIC WARNING TO SHINYHUNTERS

After the Dutch arrest, FBI Cyber Division Assistant Director Brett Leatherman addressed the group's remaining members directly. He warned that anonymity and personal relationships would not protect them and urged them to contact the FBI before investigators reached them.

The message raised the possibility that seized devices or cooperation from other members could expose the group. It also gave the remaining members a reason to question how much investigators already knew.

Leatherman referred broadly to arrests and seized infrastructure. He did not say that the FBI had seized ShinyHunters infrastructure in this case or that anyone had contacted the bureau after his warning.

Together, the two cases show different parts of the strategy. The Dutch arrest reflects the FBI's partner-led model, while the FBIJobs.gov investigation shows why the bureau relies on companies that support affected systems. No public evidence connects the arrest to the portal breach.

WHAT THE STRATEGY DOES NOT EXPLAIN

The public strategy sets priorities but does not give a timetable for carrying them out. It also does not say how quickly an organization will be contacted after the FBI finds evidence of a compromise.

The document does not explain how much technical information will accompany a warning. It also lacks public measures for judging whether earlier notifications and partner-led operations are working.

Those details will determine how much the strategy changes the experience of an organization facing an active attack. For now, businesses should prepare for earlier FBI contact without assuming how quickly a warning will arrive or what assistance will follow.

CONCLUSION

The strategy puts more weight on warning U.S. organizations while an attack can still be contained. It also allows the FBI to work through the company, agency, or foreign government best placed to act.

ShinyHunters gives the bureau an early test, but it is too soon to call the response a success. FBI support helped Dutch authorities arrest a suspected member, while the FBIJobs.gov breach remains unresolved. Investigators still have not said how the attackers gained access or whether a company supporting the portal was involved.

Businesses and critical infrastructure operators should decide who will handle FBI contact before an emergency. They also need to know where the relevant logs are stored and how evidence will be preserved. A warning can save time, but only if the organization is ready to use it.

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
 - [Aspire Managed XDR \(MXDR\)](#) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a U.S.-based team of security professionals to identify and respond to threats across a broader attack surface.
 - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced

platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
 - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire [MDR](#) delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
 - Our team of experts acts as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
 - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
 - Aspire offers [incident response services](#) to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

SUPPORTING DOCUMENTATION

[Cyber Strategy — FBI](#)

[ShinyHunters Claims FBI Breach, Says It Stole Data on Agents and Job Applicants](#)

<https://www.fbi.gov/file-repository/fbi-cyber-strategy-2026.pdf>

[FBI to ShinyHunters: 'We know how to find you'](#)

[FBI Announces ShinyHunters Arrest — FBI](#)

[FBI Statement on Compromise of fbijobs.gov Portal and Alleged Impact to FBI Employee PII — FBI](#)

[Oracle Security Alert Advisory - CVE-2026-35273](#)

[Shinyhunters · RansomLook](#)

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.