Intelligence Risk Assessment - APT29 (Cozy Bear)

Manuel Badel

Pennsylvania State University

SRA 311W SECTION 001: RISK ANALYSIS

Professor Christopher Sebora

12/1/2025

Preview

Agency Perspective: Cybersecurity and Infrastructure Security Agency (CISA)

Threat Actor: APT29 (Cozy Bear)

Primary Issue: Large-Scale Data Theft Targeting U.S. Federal Civilian Executive Branch Networks

BLUF (Bottom Line Up Front)

BLUF: APT29 (Cozy Bear) poses an immediate, strategic-level threat to U.S. national security by maintaining persistent cyber espionage operations on federal civilian executive branch networks. Three primary risks dominate the current threat landscape: (1) strategic intelligence loss that empowers Russian State goals (New Jersey Cybersecurity & Communications Integration Cell[NJCCIC], 2025), (2) operational disruption across federal agencies following compromise of interdependent systems (Wilshusen, 2009), and (3) long-term breakdown of U.S. geopolitical credibility due to the continued exposure of sensitive government information (Hamid & Huda, 2025). CISA would need to strengthen detection, continuity planning, and cross-agency data governance reforms within the next 12 months to be able to contain, mitigate and respond to this persistent threat.

Executive Summary

Executive Summary: The Russian intelligence service-sponsored threat group APT29 has enough resources to execute long-term cyber-espionage operations against federal U.S. systems. APT29 operations are known for being/having stealthy, persistent, supply-chain exploitative, tailored spear-phishing, and advanced malware (NJCCIC, 2025). APT29's main goal is highly targeted, intelligence-driven campaigns designed to extract as much sensitive and unclassified data that would directly support Russian objectives, like strategic, diplomatic, or military (Hamid & Huda, 2025).

This paper is from the perspective of the Cybersecurity and Infrastructure Security Agency (CISA) since such an organization focuses on the threat to unclassified federal civilian executive branch networks. Do not be misled by the label of “unclassified data” as these exact files contain personal information, inter-agency communications, pre-decisional policy documents, technical research, and operationally relevant data that adversaries of the U.S. can

easily weaponize against the U.S. interest (Ullah et al., 2018). Russia's intelligence services have consistently prioritized this information due to its value and the effect of strengthening Russia's global positioning, improving Russia's bargaining power, undermining U.S. alliances, and predicting U.S. actions.

Purpose of the Risk Assessment

Date of Assessment: December 1, 2025

Validity Period: This assessment is valid for 12 months (until December 1, 2026), unless a major development in Russian cyber operations, U.S. federal cybersecurity posture, or geopolitical conditions necessitates early revision.

Purpose: This intelligence risk assessment evaluates the threat posed by the APT29 (Cozy Bear) to the unclassified networks of the U.S. federal civilian executive branch agencies, mainly focusing on the risk of large-scale data theft and its implications for national, operational, and geopolitical security. It informs CISA's leadership on prioritizing identity security, cross-agency detection, and consequence management.

Three Primary Risks to the United States:

Risk 1 - Strategic Intelligence Loss Supporting Russian State Objectives: APT29 exfiltrates sensitive unclassified U.S. government information, which Russia can use to enhance geopolitical influence, predict U.S. diplomatic actions, and undermine strategic decision-making (NJCCIC, 2025; Hamid & Huda, 2025).

Risk 2 - Operational Disruption Across Interdependent Federal Agencies: Compromises in one FCEB network can have severe impacts across interconnected systems, disrupt day-to-day operations, degrade interagency coordination, and inhibit the federal government's ability to execute core missions (Wilshusen, 2009). This operational disruption stems from espionage-driven lateral movement, identity compromise, and trust degradation, not integrity or availability attacks (e.g., ransomware), which remain out of scope.

Risk 3 - Long-term Erosion of U.S. Credibility and Public Trust: Continued data theft would weaken U.S. international standing, damage trust among U.S. allies, reduce confidence in federal cybersecurity, and the immense risk of exposing sensitive internal deliberations that adversaries may weaponize for global influence (Hamid & Huda, 2025; Ullah et al., 2018).

Current Risk Status: The current level of risk is high due to the increasing operational tempo of APT29, widespread cloud adoption across federal agencies, decreasing detection times for espionage-focused intrusions, and geopolitical conditions that incentivize aggressive Russian intelligence collection.

Scope of the Assessment

Protector: The protector of this analysis is the Cybersecurity and Infrastructure Security Agency (CISA). It is the U.S. government's lead agency for the operational and technical cybersecurity defense of the country. CISA's mission is to "lead the national effort to understand, manage, and reduce risk to U.S. cyber and physical infrastructure," and CISA's vision is "a secure and resilient critical infrastructure for the American people" (CISA, n.d). CISA's statements directly target the risk of data breaches against the federal government. The point of view CISA has is that of a national-level defender since it is focused on the integrity and security of federal information and national security.

Asset: The most important and primary asset of this analysis is the confidentiality of unclassified government data, this would include personally identifiable information (PII) of millions of government employees and citizens, proprietary technical data, government agencies' sensitive information, and pre-decisional policy documents. All of these assets can directly undermine national security, economic competitiveness, and public trust in government institutions; therefore, it is of immense value to CISA. The way this data can be measured is through the volume of records stolen/breached, the sensitivity/importance of said data compromised, and the total amount of damages the event caused financially and reputationally. This analysis will NOT consider the integrity or availability of this data (example, ransomware that encrypts but does not steal any data).

Threat: The threat to the protectors in this analysis is the Advanced Persistent Threat (APT) group known as APT29 (Cozy Bear), which is attributed to the Russian Foreign Intelligence Service (SVR). Cozy Bear is a state-sponsored group that possesses sophisticated capabilities which includes advanced malware, zero-day exploits development, and sophisticated social engineering campaigns. Cozy Bear's goal is the persistent long-term espionage and extraction of intellectual property and sensitive data, mostly from Western governments, with the purpose of advancing Russia's strategic, political, and economical interests (NJCCIC, 2025). This analysis focuses on APT29, so it will consider a highly capable, patient, and well-resourced state funded threat. This scope does NOT consider any domestic insider threats, individual cybercriminals motivated by financial gain, or hacktivists. The reason the listed scope is not considered above is because the risk profile is different from a dedicated foreign intelligence service, although it is a valid threat too.

Situation: The situation is a sustained cyber-espionage campaign against the unclassified networks of U.S federal civilian executive branch (FCEB) agencies. Most of these interactions occur in the digital domain, specifically within the agency cloud environments and enterprise networks that, although protected, are still connected to the public internet to facilitate daily operations. This situation involves APT29 (Cozy Bear) gaining an initial foothold through a spear-phishing campaign or by exploiting a vulnerability in public-facing agency software. APT29 would then move laterally through the network, establish persistence, and identify and extract multitudes of sensitive, unclassified data over an extended period of time without detection. The analysis is NOT considering data theft due to the loss of a physical device, a single, isolated malware incident, or attacks targeting state, local, or private sector infrastructure.

Out-of-Scope: The following areas will not be included in this assessment: (1) Attacks on classified DoD or intelligence community networks, as it has a different security architecture and incident response authorities. (2) Insider threats, although important, insider threats operate through different access vectors and motivations (Schlicher et al., 2016). (3) Cybercriminals or financially motivated actors, this analysis focuses exclusively on state-sponsored espionage. (4) Attacks targeting state, local, tribal, or private-sector infrastructure, outside CISA's FCEB-

specific mandate. (5) Integrity or availability attacks (e.g., ransomware), the scope is limited to confidentiality and data exfiltration.

Scoping Statement: CISA faces the risk of a catastrophic compromise of sensitive unclassified government data due to a persistent and advanced cyber-espionage campaign that is conducted by the Russian state-sponsored threat group APT29 (Cozy Bear) against federal civilian agency networks.

Risk Assessment on CISA

Risk Analysis: CISA directly shapes the risk environment for the Federal Civilian Executive Branch (FCEB). CISA is responsible for securing federal civilian networks, issuing directives, coordinating incident response, and establishing baseline security standards; however, CISA does not possess operational control over each of the FCEB agencies' infrastructure. Each single agency retains authority over its own systems, creating uneven maturity levels, fragmented visibility, and inconsistent implementation of identity governance and cloud security controls. These sort of constraints are what enable APT29 to flourish since CISA's ability to enforce uniform safeguards is limited, and APT takes advantage of that.

This exact structure means the risk posed by APT29 cannot be fully mitigated by technical guidance alone. The distributed nature of the FCEB, the reliance on shared cloud identity platforms, and the partial visibility CISA receives from agencies amplify uncertainties and increase the likelihood that APT29 will maintain persistent access.

Structured Analytical Techniques Used: This risk assessment applies three complementary structured analytical techniques with the purpose of ensuring analytical rigor: Key Assumptions Check (KAC), Structured Brainstorming, and Indicators and Signposts of Change (ISC).

Key Assumptions Check (KAC) ensured that the analysis did not rely on outdated or overly positive assumptions about U.S. detection capabilities, federal interagency coordination, or Russian strategic intent. The main use of it was to ground everything on realistic outcomes and expectations, such as that several assumptions, where the expectation that agencies fully implement Zero Trust or that Russia's cyber collection priorities will diminish, were outright challenged and revised accordingly.

Structured Brainstorming was used to identify, prioritize, and categorize the three highest-impact risks to the federal civilian executive branch (FCEB). This method forced the analytic team to look beyond narrow technical issues like malware signatures, exploit mechanics, and system-level vulnerabilities and instead evaluate broader strategic and operational consequences, including the erosion of U.S. decision-making advantage, interagency disruption, and long-term damage to geopolitical credibility.

Indicators and Signposts of Change (ISC) were applied to identify observable developments that would materially shift the threat landscape over the next 12 months. Patterns such as increased Russian exploitation of cloud identity systems, accelerated credential harvesting activity, U.S. election cycles, US-Russia geopolitical escalations, and shifts in federal cybersecurity policy that would historically correlate with increased APT29 operational activity. Tracking these indicators would help anticipate when APT29 is likely to intensify espionage efforts.

Overall Risk

Overall Level of Risk: The overall risk posed by APT29 to the federal civilian executive branch (FCEB) is unambiguously high, and it will maintain that same evaluation across all three of the selected risk categories. The reason is due to it being a live, ongoing threat whose operational tempo continues to increase as geopolitical tensions rise and Russia becomes more willing to lean on its intelligence services to compensate for strategic disadvantages elsewhere (NJCCIC, 2025). The risk is elevated further when considering the simple fact that the federal agencies continue to store valuable unclassified-but-sensitive information in cloud environments that APT29 has already demonstrated the ability to infiltrate (National Security Agency [NSA], 2024). The U.S. is defending against one of the most disciplined espionage actors in the world, and CISA's defensive posture still trails behind the sophistication of Russian intrusion capabilities.

Key Assumptions: There are a total of 8 assumptions that underpin this assessment. Each assumption was evaluated for validity based on current threat intelligence, historical APT29 activity, and known defensive limitations across the federal civilian executive branch (FCEB). If

new evidence emerges, particularly in response to changes in Russian cyber tasking or U.S. defensive posture, then these assumptions should be revisited.

Assumption 1 - APT29 will continue prioritizing long-term intelligence collection over destructive operations: APT29's historical pattern of operations overwhelmingly focuses on stealthy espionage campaigns, credential theft, and persistent data exfiltration rather than disruptive or destructive activities (NJCCIC, 2025; Avertium, 2024). If Russia's strategic calculus changes, APT29 could diversify into more aggressive activity, although highly unlikely.

Assumption 2 - Federal civilian agencies (FCEB) will not reach a mature Zero Trust posture within the next 12 months: While FCEB agencies are federally mandated to adopt Zero Trust Architecture (ZTA) since President Biden's May 2021 Executive order, the organizations have made measurable progress, but full maturity remains a multi-year objective rather than an attainable near-term milestone. The NSA has identified continued reliance on legacy authentication protocols, inconsistent MFA enforcement, identity misconfigurations, and incomplete telemetry integration across cloud environments, all of which are present exploitable weaknesses for APT29 (NSA, 2024). Understanding these systematic constraints, it is reasonable to assume that there will be significant Zero Trust gaps over the next few years.

Assumption 3 - APT29 has the capability to routinely bypass or evade current federal detection technologies: APT29 regularly employs custom tooling, living-off-the-land techniques, and cloud identity manipulation that often fall below traditional detection thresholds (Avertium, 2024; NSA, 2024). APT29's continued investment in stealth supports the assumption that detection times will remain protracted.

Assumption 4 - Sensitive unclassified data will continue to hold strategic value for Russian intelligence: Though the data targeted is labeled as "unclassified," its cumulative strategic value includes PII, agency communication, policy drafts, and operational planning, all remain extremely high. Russia's documented prioritization suggests that demand for this type of intelligence will remain constant. This assumption is supported by multiple government advisories and industry reports showing that SVR-linked actors (APT 29) prioritize espionage

against government networks, and that adversaries have targeted research and U.S. government systems where sensitive but unclassified material is commonly stored (Ullah et al., 2018; NSA, 2024; NJCCIC, 2025).

Assumption 5 - Cloud environments will remain a preferred attack vector for APT29: Due to the increasing cloud adoption across federal agencies, combined with APT29's demonstrated capability to compromise cloud identity systems, it is reasonable to assume that cloud platforms will remain as a central entry and persistence mechanism for APT29 (NSA, 2024).

Assumption 6 - Geopolitical conditions between the U.S. and Russia will continue to incentivize aggressive cyber espionage: Russia has a strong motivation to intensify intelligence collection efforts due to the sanctions, military competition, diplomatic clashes, and proxy conflicts it has against the United States.

Assumption 7 - Federal agencies will continue to have uneven cyber maturity and inconsistent data governance practices: The FCEB encompasses dozens of agencies with widely varying budgets, infrastructure levels, and cybersecurity capabilities (Wilshusen, 2009; CISA, 2025). This fragmentation will continue to create exploitable entries that APT29 can leverage for lateral movement and long-term collection.

Assumption 8 - APT29 possesses sufficient resources and state support to sustain prolonged cyber-espionage campaigns: APT29 is backed by an intelligence service (SVR) with deep funding, manpower, and political protection, making it extremely unlikely that resource limitations will constrain operations (NJCCIC, 2025).

Risk Tolerance Inputs

Risk Tolerance: The United States' risk tolerance for data exfiltration by state actors like APT29 has been dangerously high for over a decade, a posture that has never been strategically viable(Wilshusen, 2009; Office of the National Counterintelligence and Security Center [NCSC], 2021). The consequences the U.S. faces for inaction range from significant to severe the range of consequences includes the degradation of U.S. diplomatic leverage (e.g., adversaries anticipating

negotiation positions), the compromise of critical intellectual property and PII of government personnel, and a fundamental erosion of trust among U.S. allies who share sensitive information with the U.S. government (Hamid & Huda, 2025; Ullah et al., 2018). CISA's current defensive posture shows that CISA accepts an unacceptable level of strategic leakage, operating on a dangerous assumption that while individual breaches are damaging, the overall system remains functional. This is a catastrophic failure of a miscalculation; the cumulative effect of these "death by a thousand cuts" incidents is a direct threat to the U.S. national security superiority. CISA and the U.S. as a whole must shift the approach from passive acceptance to aggressive mitigation; each time APT29 incurs, it is a direct counter-intelligence loss.

Historical Acceptance: Historically, the U.S. has demonstrated a troubling willingness to accept the risk posed by APT29, often reacting only after a major breach became public knowledge. The most perfect and recent example of this is the 2020 SolarWinds campaign, a massive supply-chain compromise that ended up impacting multiple federal agencies and demonstrated APT29's ability to operate with impunity for months within critical networks (NSCS, 2021). The U.S. has effectively tolerated the risk by continuing to allow the federal agencies to operate with fragmented security postures and legacy systems, creating a "patchwork of vulnerabilities" that a sophisticated actor is perfectly capable of exploiting (NSA, 2024). This historical acceptance is a luxury this great nation should no longer allow.

CISA, in coordination with the Office of Management and Budget (OMB), must compel decisive action within the next 6 to 12 months. This level of risk should not persist for a day longer than necessary as it is an abdication of CISA's core mission. The 12-month validity of this assessment is an absolute maximum window before the cumulative damage from those tiny cuts inflicts irreversible damage on U.S. strategic interests; further delay is tantamount to surrender in this silent war of cyber-espionage.

Rationale For Risk-Related Decisions

Rationale for Decisions: The rationale for prioritizing these three risks leaves no doubt, as the three risks represent a failure of U.S. cyber defense. Strategic intelligence loss is prioritized because it directly fuels adversarial decision-making. Operational disruption was selected because the very mechanisms of lateral movement and persistence degrade the trust and

coordination between federal agencies. Lastly, the erosion of credibility is a strategic, long-term poison; once allies doubt the U.S. ability to protect shared information, the U.S. global influence would wither and decay (Hamid & Huda, 2025).

Risk Outcomes and Treatment Recommendations

Uncertainties & Effect on Probability: Significant uncertainties inflate the probability and impact of these three risks. The primary uncertainty is the true scale of current, undetected compromises. APT29's mastery of "living-off-the-land" techniques directly means that CISA is underestimating APT29's presence, skewing the likelihood assessments to the optimistic side of things (Avertium, 2024). A second critical uncertainty is the speed and effectiveness of Zero Trust maturity; when agencies fall behind, the probability of breaches skyrockets. The volatility of U.S.-Russia relations is a complete wildcard; a major geopolitical escalation could push APT29 from espionage to more disruptive or devastating attacks. Due to these uncertainties, a "High" likelihood to all three risks should be assigned, especially if the base of the assessment is on the assumption that the defenses are fully effective would be professionally negligent.

Strategic Intelligence Loss - Risk 1 - Treatment(Mitigate): The U.S. cannot avoid the threat of a state-sponsored group like APT29 (Cozy Bear)**,** the loss of such sensitive data should not be accepted. The primary focus should be aggressive mitigation through an accelerated and uncompromising implementation of Zero-Trust principles. More specifically, CISA must mandate the elimination of legacy authentication protocols on all remaining FCEB agencies that have not updated policy, within the next 6 months, as these are the primary attack vector for APT29 cloud access campaigns (NSA, 2024).

Operational Disruption - Risk 2 - Treatment(Mitigate): The goal is to sever APT29's ability to move laterally and disrupt operations. This would require mandating and enforcing a strict identity and access management (IAM) control set across all of the FCEB agencies, focusing on universal, phishing-resistant multi-factor authentication (MFA) and just-in-time admin access (JIT). The hope that agencies would do this voluntarily is a proven mistaken belief (Wilshusen, 2009). CISA must ensure its authority to mandate these controls, leveraging its continuous

diagnostics and mitigation (CDM) program to actively monitor and enforce compliance, leading to a containment of breaches to initial entry points.

Erosion of U.S. Credibility and Trust - Risk 3 - Treatment(Transfer/Mitigate): This is one of those risks where it might not seem as important at first glance, but when taking a step back and looking at the potential consequences, one can infer that this risk cannot be accepted, and avoiding it completely is also impossible. Therefore, transferring a portion of the financial and operational risk through robust cyber insurance for the federal government and mitigating the reputational damage through a proactive, transparent crisis communication plan. By following these steps and having a pre-established, White House-coordinated plan to swiftly and confidently inform allies and the public about breaches, controlling the narrative and demonstrating competence even in failure is extremely important to preserve the trust of the people.

Consequence Management Plan

Immediate Containment Protocol: Upon confirmation of a major APT29 breach, CISA must immediately activate the National Cyber Incident Response Plan (NCIRP), transitioning from a defensive to a wartime footing. The first 72 hours are critical, as the primary objective is the expulsion of the adversary and the stabilization of federal networks. This would require a mandatory, government-wide directive to isolate compromised identity providers, particularly in cloud environments, which APT29 heavily targets (NSA, 2024). A mass credential reset for all federal civilian executive branch personnel is non-negotiable, despite the significant operational disruption. This action would sever APT29's primary persistence mechanism, which is stolen credentials (NJCCIC, 2025). At the same time, CISA hunt teams must deploy to the most critically impacted agencies to perform forensics analysis, identify the full scope of the data exfiltrated, and ensure the adversary is fully evicted.

Crisis Communication Strategy

Communication with U.S. Allies: The moment a breach is confirmed, the Secretaries of State and Defense must initiate confidential, direct calls with key allied counterparts. These calls must occur before any public announcement, and the messaging must be transparent and reassuring: A

proactive, confidential briefing is the only way to preempt the corrosive speculation and distrust that APT29's actions are designed to create.

Communication with the American Public: A public announcement must be delivered by a unified voice, ideally someone of high standing like the Secretary of Homeland Security, within 24 hours of containment. The message the individual gives must be clear, the statement must emphasize the immediate steps taken to secure systems and protect data, directly address public fears about personal information. It is of great importance to make sure not to downplay or obscure the severity of the event, as that could destroy what remains of public trust in federal cybersecurity.

Communication with Congress: Briefings to relevant congressional oversight committees must be timely, factual, and avoid political blame-shifting. The focus must remain on the nature of the foreign threat, the effectiveness of the response, and the path going forward.

Summary with Specified Recommendations

Summary: The persistent threat posed by APT29 represents a clear and present danger to national security that demands immediate action. This Russian state-sponsored group continues to exploit systemic vulnerabilities within federal civilian networks, creating three critical risks: the ongoing theft of strategic intelligence that directly empowers Russian objectives (NJCCIC, 2025), operational paralysis stemming from espionage activities (Wilshusen, 2009), and irreversible erosion of U.S. credibility and public trust (Hamid & Huda, 2025). The treatment plans focusing on data-centric security, enforced identity controls, and consequence management, provide a viable path to defeat APT29.

Direct Recommendation: The single most impactful action is the immediate prioritization and funding of the mitigation plan for Risk 1: Strategic Intelligence Loss. This plan directly counters APT29's core mission. CISA must issue a binding Emergency Directive mandating the implementation of data-centric security models, specifically leveraging frameworks like the MESA security model 2.0 to tag, track, and encrypt sensitive data (Singh & Afzal, 2024). This action moves the goalpost on APT29; the objective is to render exfiltrated data useless to

Russian intelligence, thereby destroying the operational value of APT29's espionage campaigns and protecting the nation's decision-making advantage. This initiative does require a considerable amount of funds for CISA's "Data Centric Security" plan. It also requires temporary emergency authorities from Congress, granting CISA the power to mandate implementation across all FCEB agencies, overriding bureaucratic inertia. This initiative would likely take an 18-month mandatory sprint to achieve foundational implementation. The 12-month validity of this assessment marks the period of most acute and unaddressed risk, a direct result of past inaction. The 18-month timeline reflects the stark reality of remediating a decade of neglected federal cybersecurity architecture. Significant risk reduction must be demonstrated within the first 12 months, including the mandatory elimination of legacy authentication protocols and the encryption of all high-value data sets to prevent further catastrophic loss. The full 18-month horizon is non-negotiable to achieve the level of maturity, a data-centric posture would require to permanently raise the cost of espionage for APT29.

Appendix

Risk Scorecards and Final Risk Matrix for APT29 (Cozy Bear) - CISA Perspective

(OpenAI, 2025)

Risk	Description	Likelihood (1–5)	Impact (1–5)	Overall Rating (L × I)	Justification (Why These Scores?)	Recommended Treatment
Risk 1: Strategic Intelligence Loss	Persistent espionage allowing Russia to exfiltrate sensitive unclassified federal data supporting their geopolitical and intelligence goals.	**5 – Very High**	**5 – Very High**	**25 (Extreme)**	APT29 history shows long-term, stealthy, state-backed collection, including SolarWinds. High value of PII, policy drafts, interagency communications makes this a priority target.	**Mitigate + Avoid** (Identity hardening, Zero Trust acceleration, cross-agency data governance).
Risk 2: Operational Disruption Across Interdependent Agencies	Compromises allow lateral movement across FCEB networks, degrading mission execution and interagency coordination.	**4 – High**	**4 – High**	**16 (High)**	Uneven cyber maturity across FCEB agencies increases probability. Disruption arises indirectly from espionage activity, not destructive attacks.	**Mitigate + Transfer** (Shared responsibility models with cloud vendors; mandated minimum-config baselines).

Risk 3: Long-Term Erosion of U.S. Credibility & Public Trust	Repeated compromises degrade confidence of allies, damage U.S. diplomatic leverage, and undermine public trust in federal cyber defense.	**4 – High**	**5 – Very High**	**20 (Very High)**	Data theft revealing internal deliberations undermines global reputation; long-term strategic harm exceeds immediate technical loss.	**Mitigate + Accept (Partially)** (Communications strategy, international reassurance, transparency after breaches).

Likelihood ↓ / Impact →	**1 Low**	**2 Moderate**	**3 Significant**	**4 High**	**5 Very High**
5 – Very High	5	10	15	20	**25 – Risk 1 (Strategic Intelligence Loss)**
4 – High	4	8	12	**16 – Risk 2 (Operational Disruption)**	**20 – Risk 3 (Credibility & Trust Erosion)**
3 – Medium	3	6	9	12	15
2 – Low	2	4	6	8	10
1 – Very Low	1	2	3	4	5

Interpretation of Matrix Placement

Risk 1 = Extreme (25): Must be addressed immediately within 12 months.

Risk 2 = High (16): Requires mandatory agency action and CISA enforcement mechanisms.

Risk 3 = Very High (20): Requires strategic leadership involvement and international communication plans.

References

Avertium. (2024). *Evolution of Russian APT29: New attacks and techniques uncovered*. https://www.avertium.com/resources/threat-reports/evolution-of-russian-apt29-new-attacks-and-techniques-uncovered

Cybersecurity and Infrastructure Security Agency. (n.d.). *About CISA*. https://www.cisa.gov/about

Hamid, S., & Huda, M. N. (2025). Mapping the landscape of government data breaches: A bibliometric analysis of literature from 2006 to 2023. Social Sciences & Humanities Open, 11, 101234. https://www.sciencedirect.com/science/article/pii/S2590291124004315

National Security Agency. (2024). *Russian SVR cyber actors adapt tactics for initial cloud access* (Joint Cybersecurity Advisory). U.S. Department of Defense. https://media.defense.gov/2024/Feb/26/2003399756/-1/-1/0/CSA-SVR-ADAPT-TACTICS-FOR-INITIAL-CLOUD-ACCESS.PDF

New Jersey Cybersecurity & Communications Integration Cell. (2025). *Russia – APT29 threat profile*. https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/russia-cyber-threat-operations/russia-apt29

OpenAI. (2025). *ChatGPT (Version 5.1)* [Large language model]. https://chat.openai.com/

Office of the National Counterintelligence and Security Center. (2021, August 19). *SolarWinds Orion software supply chain attack*. U.S. Government. https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/SolarWinds%20Orion%20Software%20Supply%20Chain%20Attack.pdf

Schlicher, B. G., MacIntyre, L. P., & Abercrombie, R. K. (2016). Towards reducing the data exfiltration surface for the insider threat. Oak Ridge National Laboratory. https://www.osti.gov/servlets/purl/1328274

Singh, S. P., & Afzal, N. (2024). The MESA Security Model 2.0: A dynamic framework for mitigating stealth data exfiltration. International Journal of Network Security & Its Applications, 16(3), 23– 41. https://arxiv.org/pdf/2405.10880

Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, M. A., & Rashid, A. (2018). Data exfiltration: A review of external attack vectors and countermeasures. Journal of Network and Computer Applications, 101, 18–54. https://www.sciencedirect.com/science/article/pii/S1084804517303569

U.S. General Services Administration. (2022). *APT buyer's guide* (Version 2). https://www.gsa.gov/system/files/APT_Buyers_Guide_v2_July_2022.pdf

Wilshusen, G. C. (2009). Cyber threats and vulnerabilities place federal systems at risk (Testimony before the House Committee on Oversight and Government Reform). U.S. Government Accountability Office. https://www.gao.gov/assets/gao-09-661t.pdf