SYM-AM-24-032

Excerpt from the Proceedings of the Twenty-First Annual Acquisition Research Symposium

Acquisition Research: Creating Synergy for Informed Change

May 8–9, 2024

Published: April 30, 2024

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

The research presented in this report was supported by the Acquisition Research Program at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

ACQUISITION RESEARCH PROGRAM
DEPARTMENT OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

Vulnerabilities and Social Engineering in Acquisition Scenarios

Clayton Boyer—is a Principal Acquisition Program Manager at the MITRE Corporation who supports DoD, Intel, and Federal sponsors throughout their acquisition life cycles. His focus is on cloud and complex IT acquisitions, as well as supply chain risk management. He has over 16 years of experience in acquisition and contracting, with 14 years as a Civilian in the Intel Community as a Contracting Officer and Program Manager. He holds a bachelor's and master's in business administration, with concentrations in management information systems and information security, respectively.

Mary Evans—is a Principal Decision at the MITRE Corporation. She supports Civilian and Defense sponsors in acquisition strategy, source selection facilitation, and protest support. She assists sponsors in adopting innovative technologies and acquisition strategies to reduce the burden of procurement activities, and risk of successful award protests, and shorten the overall time-to-award. Evans has over 20 years of experience in acquisition support and 15 years in IT service management and program management. She holds a BS in accounting from George Mason University and numerous IT industry certifications.

Kathleen Hyatt—is a Lead Systems Engineer at the MITRE Corporation who supports Intelligence Community, Defense, and Federal sponsors throughout all phases of the acquisition life cycle including systems development. She has more than 12 years of experience in acquisitions and systems engineering. She holds an MS in systems engineering, George Washington University; an MS in accounting and finance management, University of Maryland; a BA in English, University of Maryland; and a certificate in procurement and contracts management, University of Virginia.

Terry Leary—is an Acquisition Principal at the MITRE Corporation who supports Intelligence Community, Defense, and Federal sponsors with their acquisition strategies and source selections. He has more than 30 years of experience in program management, acquisition, and contracting. He is a former Air Force Program Manager and Engineer for major systems acquisitions. He holds an MS in astronautical engineering from George Washington University and a BS in astronautical engineering from the U.S. Air Force Academy.

Zack Levenson—is a Senior Contract Analyst at the MITRE Corporation who supports Intelligence Community, Defense, and Federal sponsors throughout their acquisition life cycles. His interests include security and counterintelligence risk associated with the acquisition and contracting practices of the federal government. He has 5 years of experience in acquisition and contracting and is a former Subcontract Administrator. He holds a BA in political science from West Virginia University and a certificate in contract management from Villanova University.

Ryan Novak— is an Acquisition Outcome Lead at the MITRE Corporation and AI Lead for Acquisition Innovation Center, has earned two MBAs, an MS in strategic purchasing, an MS in project management, and is DAWIA III Contracting certified. He has authored the Challenge-Based Acquisition Handbook, taught the approach to 500+ staff at MITRE, Industry, and the Government, and helped numerous agencies employ innovative acquisition approaches. He is a former USAF Contracting Officer with 28 years of leadership experience. He is a published author, speaker, and practitioner on innovative acquisition approaches and solutions. He has helped achieve strategic program and acquisition successes for the DoD, Civilian Agencies, and the IC across the board.

Abstract

As our adversaries look to weaken the United States, a constant barrage of social engineering attacks are hitting both the Defense Industrial Base and the Government at record numbers. Constantly, our adversaries are looking for weaknesses within our acquisition system to collect information, conduct fraud, or steal U.S. Government funded intellectual property. The report entitled "Vulnerabilities and Social Engineering in Acquisition Scenarios" is a follow-up effort to the paper presented by MITRE at the NPS Acquisition Research Symposium in May 2023, "Social Engineering Impacts on Government Acquisition." We have developed hypothetical scenarios

based on open-source reporting where our government acquisition community is uniquely vulnerable and susceptible to attacks. Each scenario aligns to a different part of the acquisition lifecycle and addresses various social engineering attack and compromise types. These scenarios highlight different government agencies and various acquisition positions (e.g., contracting officer, program staff, technical members of source selection panels, contracting specialists, etc.) to demonstrate how different mission sets and roles can all be affected by acquisition exploitation. We discuss the impact of each vulnerability attack, whether that be economic espionage or exposure of CUI. Finally, each scenario includes recommendations that can be used to help mitigate the risk, decrease the attack surface, or repel a future attack.

Introduction

The Federal acquisition workforce is becoming increasingly vulnerable to intelligence collection and exploitation attacks, to include social engineering attacks, information exploitation, and malign influence. The nature of acquisition procedures encourages the open sharing of data across internal and external stakeholders. The nature of acquisition is to encourage participation and competition from all U.S. businesses, no matter the socio-economic status, current relationship with the Government, or location. This puts the acquisition workforce in a uniquely vulnerable position when conducting routine acquisition activities such as market research, which requires receiving and disseminating email attachments (MITRE ATT&CK, n.d.-d) from unknown companies. When combined with heavy workloads and manual processes, both of which increase the potential for human errors, it creates an environment where acquisition staff present themselves as targets ripe for attackers to exploit.

The Federal acquisition process introduces a myriad of potential attack opportunities for U.S. adversaries to exploit in their efforts to infiltrate U.S. critical supply chains in their pursuit of global economic superiority. Acquisition is a complicated process occurring largely on unclassified networks with many different stakeholders playing key roles throughout the lifecycle. This, in combination with the fact that acquisitions coalesce and share massive amounts of data in order to comply with the "Competition in Contracting Act," creates a unique and currently under-addressed situation in which acquisition staff across industry and government have become rich targets for exploitation. There is growing evidence demonstrating the extent that our adversaries are exploiting the U.S. Government (USG) and its Industrial Base in any way possible, while awareness of the issue lags far behind. Most USG agencies do not have acquisition policies and processes to adequately address this threat.

In an effort to demonstrate areas where the government acquisition community is uniquely vulnerable, the following hypothetical scenarios were developed to help show potential types of attacks, potential impacts of attacks, and recommendations to assist in mitigating or repelling such attacks. Each scenario aligns to a different part of the acquisition lifecycle and addresses various social engineering attack and compromise types. These scenarios highlight diverse government agencies and many acquisition positions (e.g., contracting officer, program staff, technical members of source selection panels, contracting specialists, etc.) to demonstrate how the mission sets and roles can all be affected by acquisition exploitation.

The intent of these scenarios is to increase awareness of potential issues within the acquisition community and help acquisition professionals recognize when they are potential targets. With awareness will come increased security practices and processes that will help to limit the effects and vectors for potential acquisition exploitation and social engineering attacks against the government acquisition community.

Definitions

Artificial Intelligence (AI): The practice of programming and utilizing machines to mimic human intelligence to perform tasks (McKinsey & Company, 2023).

Machine Learning: The act of developing artificial intelligence through models that can "learn" from data patterns without human direction. Machine learning is a type of artificial intelligence (McKinsey & Company, 2023).

Operational Technology (OT): Programmable systems or devices that detect or cause a direct physical change in a system or environment. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms (Editor, n.d.). OT systems are often not designed to be internet connected and run on proprietary software. OT differs from IT because IT systems are designed to be networked and typically run commercially available operating systems like iOS and Windows, which are more secure as they are broadly monitored and continuously updated.

Social Engineering: The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust (National Institute of Standards and Technology, 2023).

Attack/Compromise Type

AI Bias: The fact that any outputs, judgements, or answers provided by AI are inherently based on the data that the AI engine was taught, learned, and trained on. AI technology is 100% reliant on source data such as news articles, magazines, scholarly journals, books, and many other types of media to leverage as "knowledge." Furthermore, humans decide which type of data that is ingested by the model. Therefore, AI may give answers that unfairly discriminate against, or in favor of, particular individuals or groups if the sources that underpin the AI technology contained bias (Team, n.d.).

Client/Vendor Impersonation Fraud: This technique involves a social engineer posing as a client or vendor in order to gain sensitive information through a conduit of trust; phishing and other techniques can be used to collect information to build a more sophisticated cover-for-action and cover-for-status.

Cold Calling/Vishing: This technique involves a simple act of gathering information by making unsolicited phone calls, sending voice messages, and leaving voicemails as a means to make contact. These acts are conducted in ways that initially seem to amount to insignificant interactions, but small pieces of information about a person gathered separately over time are often combined to form a valuable profile to be used by attackers.

Elicitation: This technique involves a subtle approach that is used to gather information from users through basic social interactions and research into a user's online and social media presence.

Framing: This technique is used to frame a situation by asking leading questions or phrasing statements in such a way that they focus on the target's unique biological and cultural influences to create a level of comfort and familiarity. That familiarity is then leveraged to manipulate targets into sharing sensitive information or enabling access to systems.

Phishing: This technique is one of the most popular social engineering attack types, which are email and text message campaigns aimed at creating a sense of urgency, curiosity, or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware (MITRE ATT&CK, 2020).

Pretexting: This technique is a premeditated attack in which a person constructs an elaborate story to place a user in a tense and urgent situation in which they might disclose information they normally would not disclose.

Spear Phishing: This technique is a type of phishing attack that targets specific individuals or organizations, typically through malicious emails. The goal of spear phishing is to steal sensitive information such as login credentials or infect the targets' device with malware. Spear phishers carefully research their targets, so the attack appears to be from trusted senders in the targets' life (CrowdStrike, 2023).

Scenario 1: "Open Source" Acquisition Data Collection

Acquisition Phase(s): Market Research, Solicitation

Attack/Compromise Type: Framing, Pretexting, Cold Calling/Vishing, Vendor Impersonation

Scenario: A foreign agent, posing as a business development manager for a small business, creates accounts on sites like SAM.gov and gains access to Requests for Proposals (RFP) and Requests for Information (RFI) from USG Agency solicitations that mention Operational Technology (OT) engineering (e.g., traffic lights, water plant control systems, railway control systems, etc.). The agent canvases the POCs listed in the RFPs and RFIs to gain access to additional solicitations – under the guise of obtaining business opportunities for their fictional company (MITRE ATT&CK, n.d.-f).

By compiling several solicitations and RFIs, the foreign agent begins to piece together critical information (MITRE ATT&CK, n.d.-c) on USG capabilities, to include:

- The offices and departments working OT based projects
- The scope and size of OT needs the USG Agency has (e.g., number of full-time equivalents [FTEs] requested/relative budgets of specific offices, etc.)
- The technical focus areas where the USG Agency needs assistance (e.g., agency problems identified in the Statement of Work [SOW] may outline where the USG staffing or technical capability is currently lacking)

Potential impact: By compiling many pieces of seemingly inconsequential unclassified information in acquisition documentation, a foreign agent could compile a profile of USG Agency focus areas in the OT space. The level of detail of the agent's report would directly correlate to the detail in acquisition documents, which is often extensive, to allow companies to accurately bid on projects.

The nature of the USG Agency's mission – protecting U.S. infrastructure – combined with the OT-focused acquisition documents, would allow the foreign agent to deduce potentially harmful vulnerabilities and allow the foreign actor's government to invest/focus on areas where the United States is most exposed. By nature, OT has direct physical impacts on systems or environments and, if exploited, could pose real-world harm.

Recommendation: Agencies should move towards publicizing acquisition information in tightly controlled portals that are actively administered and monitored. For agencies without separate networks for sensitive (i.e., Personal Identifiable Information [PII]/Protected Health Information [PHI]) or classified information, a request should be made to receive the RFI from the Contracting Officer (CO). This will still meet fair competition requirements without publicly releasing acquisition information, and all Federal/State/Local governments should follow similar models to reduce their exposure to these "open source" type attacks.

Scenario 2: AI-Enhanced Market Research

Acquisition Phase: Market Research

Attack/Compromise Type: AI Bias

Scenario: In an era marked by technological advancement, a USG Agency has embraced the integration of Artificial Intelligence (AI) into their acquisition processes, particularly in the pre-award market research phase. Leveraging AI can augment and expedite the work of the Acquisition Team. The USG Agency collects and analyzes vast amounts of data from various sources, including industry reports, supplier databases, and other market analysis platforms. This AI-driven approach allows them to identify potential vendors, trends, the current state of technology, potential solutions, acquisition approaches, and cost-saving opportunities with unprecedented speed and accuracy.

In the pursuit of acquiring next-generation Humvees, the USG Agency has embraced AI-driven market research to identify potential suppliers with a proven track record of durability and ruggedization. The CO relies on AI-based analysis to sift through vast amounts of data, aiming to identify companies known for their exceptional capabilities and innovative solutions in these areas. However, a devious plot unfolds when U.S. Automaker #1, a contender for the contract, decides to tarnish the digital reputation of its closest competitor, U.S. Automaker #2. U.S. Automaker #1 launches a comprehensive campaign to inject negative bias (MITRE ATLAS, n.d.-a) into the AI models and data sources that provide information, evidence, and support to the USG Agency's market research and overall acquisition decision-making process.

U.S. Automaker #1 initiates a covert digital marketing campaign aimed at discrediting U.S. Automaker #2. They flood the internet with poorly reviewed blog posts, YouTube videos, Facebook reviews, Instagram posts, and other content that portrays U.S. Automaker #2's Humvees as unreliable and unsafe. These misleading narratives aim to manipulate public perception. They also finance biased research studies carefully designed to highlight flaws in U.S. Automaker #2's Humvees. These studies are strategically published in reputable journals and magazines, lending an air of credibility to the misinformation. The disinformation creates a snowball effect of negative publicity, studies, and social media posts.

Ultimately, this leads to a severe decline in U.S. Automaker #2's Humvee sales, severely impacting their reputation. Meanwhile, the AI algorithms processing market data "ingest" these indicators of low quality and durability, further exacerbating the bias against U.S. Automaker #2 in the USG Agency's AI-driven market analysis.

Potential Impacts: By manipulating the USG's AI-driven market research, companies can influence the acquisition process and gain a competitive edge, resulting in awards to vendors who may not have the best interests of national security at heart and/or may not be the "best" vendor that provides the "best" solution for the USG Agency. This could lead to the acquisition of subpar or potentially even compromised technology and reduce the Defense Industrial Base, jeopardizing this or other mission-critical operations.

This scenario can also be flipped, and instead of injecting negative bias towards a competitor, a company can inject positive bias, artificially inflating their own reputation, products, and solutions to gain a competitive edge over other vendors.

Recommendations: To safeguard against these vulnerabilities in AI-enhanced market research, government agencies should consider implementing enhanced authentication. They should implement stringent authentication and verification processes for access to AI-driven market research platforms and ensure that only authorized personnel and vetted firms can contribute to the AI data pool. Agencies should continuously audit AI algorithms for anomalies and should institute rigorous data protection measures to prevent unauthorized access and maintain human oversight in the AI-driven process to critically evaluate recommendations and trends generated by the AI. Humans can provide context and judgment that AI may lack; therefore, a close collaboration between the Acquisition and Technical teams is imperative to ensure market analysis aligns with actual technical requirements. Finally, agencies should

continuously educate the Acquisition Team on the risks of AI as a whole and train them to identify potential threats and signs of bias injection.

Agencies should monitor digital platforms for suspicious campaigns and disinformation activities and continuously collaborate with cybersecurity experts to detect and mitigate these threats. These recommendations can allow agencies to tap into the power of AI while mitigating the risks of compromise and exploitation by nefarious actors.

Scenario 3: Market Research Information Gathering

Acquisition Phase(s): Market Research, Solicitation

Attack/Compromise Type: Client/Vendor Impersonation Fraud

Scenario: A malicious actor identifies the government program manager (PM), teammates, and the likely acquisition timeline for a major enterprise acquisition for the USG Agency during an Industry Day that was published on SAM.gov (MITRE ATT&CK, n.d.-f). The contract specialist (CS) publishes his USG email address on SAM.gov to coordinate attendance. The USG Agency is utilizing a full and open competition for this solicitation, so there are several companies inquiring who are unfamiliar to the CS. Further, the CS is extremely busy with preparing the solicitation package and coordinating the Industry Day. In conjunction with the Industry Day, the USG Agency posts an RFI to give Vendors the opportunity to provide feedback on the materials to be presented during the Industry Day.

Unfortunately, and unbeknownst to the CS, the malicious actor submits an email response to the RFI with a PDF attachment that contained malware (MITRE ATT&CK, n.d.-d). With all the active distractions happening at once, the malicious email did not get the security scrutiny that it should have by the CS. Without knowing, the CS has unknowingly forwarded a malicious attachment to the entire technical program team, which later results in a backdoor providing unauthorized access into the USG Agency network.

Potential impact: With the program hierarchy information gleaned from the Industry Day and the backdoor access provided by the malicious attachment, the agent proceeds to systematically comb through USG Agency systems and databases, downloading and exfiltrating gigabytes of valuable health records, personnel files, and military duty summaries for thousands of patients.

From these sensitive records, the malicious actor is able to piece together sensitive operational details of several military operations – based on the patients' skill identification codes, educational histories, and their combat injuries. The actor is able to use all of this information to piece together how many different units assemble their teams and operate in combat.

In addition, the actor is able to report back to their home country with large amounts of PII on patients who operated in the actor's home country or in operations where the home country was a target. They are able to build a roster of U.S. personnel to target in future retribution operations.

Recommendation: Agencies should move towards publicizing acquisition information in tightly controlled portals that are actively administered and monitored. Vendors should be required to register for the portal and undergo a verification process before gaining access. Each RFI/RFP published should also be limited based on 'need-to-know.' Companies should be required to prove via North American Industry Classification System (NAICS) codes or prior experience that they have expertise that is applicable to the RFI/RFP before gaining access. All of these measures still allow for fair competition while also verifying Vendors and reducing the risk of malicious actors accessing sensitive information.

Scenario 4: International Traffic in Arms Regulations (ITAR)/Controlled Unclassified Information (CUI)

Acquisition Phase(s): Solicitation, Contract Management

Attack/Compromise Type: Cold calling/Vishing (Donahue, n.d.), Client/Vendor Impersonation Fraud

Scenario: ITAR is a regulation established to restrict and control the export of defense and military related technologies to safeguard U.S. national security and foreign policy objectives. This regulation is in place so that when the need arises to share technical data outside of the United States with its partners, it is approved for sharing by the USG to export the material or information to a foreign person who has the appropriate need-to-know (Article – DDTC Public Portal, 2016). Acquisition and solicitation documents may contain sensitive information that should only be shared with approved ITAR partners.

An RFP is published containing information about new technology regarding equipment being developed by the USG Agency. A CS involved in the creation of the RFP is contacted by someone claiming to be from one of the bidding companies, when in actuality, this person is an imposter attempting to access sensitive contract information. The imposter requests to view the full solicitation/RFP package and the details on the new USG Agency technology and equipment. The RFP materials are marked as ITAR/CUI sensitive, and the unknown entity claims to be a representative from a company with prior ITAR approval. ITAR approvals for companies must be renewed every 12 months. The CS, who is unfamiliar with ITAR regulations, is overtasked during the RFP/solicitation phase of the acquisition. The imposter posing as a representative from the company states that the company is approved for ITAR sharing, but the CS fails to notice that the approval in question expired the prior month. The CS then grants the request and sends the RFP containing the sensitive data to the foreign entity, thereby sharing information in a way that does not comply with ITAR regulations.

Potential impact: The RFP contains information on how to develop USG Agency owned property, which is exposed to a non-U.S. entity. This data is exported in violation of state department and export rules, which creates the potential for the adversary to duplicate/steal the technology, or even for them to find access points into the equipment to possibly disrupt future missions.

The request to share information with external entities can arise during the contract management phase as well, after the contract has been awarded. Contract professionals must be aware of ITAR regulations in order to answer these requests throughout the entire acquisition lifecycle.

Recommendation: ITAR is not a topic that comes up often during the acquisition process. Agencies should strive to increase awareness of ITAR regulations and policies, as some contracting and acquisition professionals may not be familiar with them or the process for sharing information with entities and partners external to the United States. Further, agencies should consider adding a step into the solicitation process to double check the recency of ITAR approval for all bidding companies.

Scenario 5: Economic Espionage

Acquisition Phase(s): Solicitation

Attack/Compromise Type: Framing, Pretexting (Donahue, n.d.), Cold Calling/Vishing (Donahue, n.d.), Client/Vendor Impersonation Fraud

Scenario: A foreign agent, posing as a lead researcher in a company that develops vaccines, tricks a CS into sharing Government Furnished Information (GFI) associated with a vaccine development solicitation that is currently "on the street." The GFI contains key information gleaned from years of intensive research and millions of dollars spent, thereby enabling Intellectual Property Theft for the purpose of boosting a Nation State's economic interests.

With the advent of hybrid work models, the foreign agent is able to target hundreds of CSs across the country supporting vaccine-adjacent programs. Using common business platforms, the agent is able to reach many more targets with minimal time and effort invested.

Potential impact: Gaining access to key research findings allows the foreign agent to convey valuable insights back to their government to be exploited. The foreign government is able to forego investing years of time and money into developing their own vaccine and use state-owned companies to begin producing the U.S. vaccine ahead of other manufacturers.

While the vaccine is successful in saving many lives, the foreign government also sells it to several other countries, reaping massive profits across the world. The U.S. companies who invested in the vaccine miss out on millions of vaccine sales and are unable to recoup their research and development costs. This leaves them less financially able to continue research and development on future vaccine initiatives. Future diseases end up taking longer to thwart, as the leading vaccine company from the foreign country has no research/development capabilities.

Recommendation: Agencies should move towards keeping active control of critical data, even if it is not classified or national security related. Maintaining lists of trusted entities, whom GFI or other critical information can be released to, would be highly recommended. Companies participating in solicitations would provide POC lists to the CO, and all government personnel should refer to the list before the release of *any* information, especially critical GFI or background data.

For an even more robust response, the government should consider creating dedicated IT systems for contractors to view and consume critical GFI or other agency-owned information without being able to export or remove the information from those systems. Vendors could then build proposals with knowledge of the critical information, but the official records/databases/documents would remain close hold. Software development sometimes occurs in this manner. The government provides an entire IT system for developing code, that is entirely hosted and controlled by the government, then the contractor performs their work on the government systems, not a contractor system, thereby ensuring the government retains control of critical data and interfaces.

Scenario 6: AI-Enhanced Source Selections

Acquisition Phase: Source Selection

Attack/Compromise Type: AI Bias

Scenario: A USG Agency is in the process of procuring an advanced border surveillance system to enhance national security. To expedite vendor selection, the USG Agency has incorporated AI into the evaluation process, allowing AI algorithms to analyze and rank potential vendors based on predetermined evaluation criteria such as cost, technical expertise, and past performance. However, this innovative approach inadvertently leads to AI-induced bias in the vendor selection process, with potentially far-reaching consequences.

In an effort to streamline the vendor selection process, the USG leverages AI to assist in the evaluation of proposals submitted by potential contractors. The AI system processes vast amounts of data, including both sections L and M, past performance records, technical

capabilities, and cost estimates to assess each vendor's suitability for the project. This approach has the potential to enhance efficiency and objectivity in the evaluation process.

Unbeknownst to the agency, there is a flaw in the AI's training data (MITRE ATLAS, n.d.-b). The flaw concerns the past performance data for the vendors. Though the system should be considering past performance data from the past 5 years, the AI engine's training model only contained data for 2 of the last 5 years because it hadn't been updated since 2021. This effectively disregards several years of data that could impact the overall assessment of a vendor and their ability to successfully deliver on the contract requirements.

This systematic flaw introduces unintended bias into the system. The inaccurate historical information that was used to train the AI model creates an inadvertently lower score assigned to proposals submitted by small businesses, even though they possess competitive technical capabilities and cost-effective solutions. This bias results in the unintentional exclusion of highly qualified small-business vendors from the shortlist of potential contractors. These vendors, despite meeting all the specified criteria, consistently receive lower rankings due to the biased AI evaluation.

Potential Impacts: This AI-induced bias leads to the unjust exclusion of qualified vendors, potentially limiting the government's access to innovative and cost-effective solutions. Furthermore, it erodes trust in the fairness of the acquisition process, raising concerns about bias in AI-driven decision-making within the USG Agency. Also, it could impact the solution that is acquired and the overall mission of the Agency.

Recommendations: The USG should ensure that the AI's training data is comprehensive, diverse, and free from historical biases. They should employ continuous monitoring and validation of the training data as this could help mitigate the risk of bias. Also, the USG Agency should maintain a human oversight mechanism in the evaluation process. Expert evaluators should review AI-generated recommendations, correcting any instances of bias and ensuring that decisions align with the Agency policies.

Scenario 7: Technical Exchange Panel (TEP)

Acquisition Phase(s): Source Selection

Attack/Compromise Type: Elicitation, Spear Phishing (MITRE ATT&CK, n.d.-d)

Scenario: During an Industry Day for an upcoming solicitation, a foreign actor (agent) identifies the program lead and teammates and the likely timeline for a major USG acquisition. The agent then turns to social media to develop an initial profile of each of the team members, including personal email accounts (MITRE ATT&CK, n.d.-b). The social media research leads the agent to see that the program lead's daughter is part of a travel softball team and there are many photos on Facebook. The agent then poses as a photographer from a local newspaper and crafts an email to the program lead's personal email including a link to additional photos from a recent game. The program lead clicks on the link using his personal phone, not realizing the link contains malware that allows the agent to exploit a software vulnerability and install a backdoor on the program lead's iPhone. This allows the agent to bypass authentication and control the phone remotely.

For the next few weeks, the agent uses the microphone on the iPhone to listen in (MITRE ATT&CK, n.d.-a) on virtual technical exchange panel (TEP) deliberations on technical merit, risks, and impact, discussions of the elements and realism of the business proposals, and the trade-offs between technical merit, risk, and price. All information that can be used by the agent to collect mission critical information.

Potential impact: By listening in on the USG TEP consensus session, the competitor/foreign agent gains more nuanced information to add to what is publicly available. There are numerous applications in obtaining this inside information. This ranges from simply gaining an unfair competitive advantage in accessing a proposal or leakage of intellectual property (IP) and its value as perceived by the government to an industry competitor conducting full-scale IP theft. Full scale IP theft could boost a nation-state's economic interests by allowing it to avoid research and development investments.

Recommendations: Agencies should resist prevailing post-COVID practices of remote consensus sessions and prohibit phones. Additionally, the USG should add social engineering training to procurement integrity training and conduct the training at key phases of the acquisition schedule. Finally, it is recommended that they ensure all key stakeholders both in industry and government practice cyber hygiene and proper mitigations are put in place at home, outside, and in the office to resist simple cyber-attacks that can compromise information.

Scenario 8: Consensus

Acquisition Phase(s): Source Selection

Attack/Compromise Type: Elicitation

Scenario: A large oil company located in the Middle East finds a government solicitation on SAM.gov (MITRE ATT&CK, n.d.-f) for overseas fuel replenishments. This oil company is nation-state backed by a kingdom that is looking to improve their diplomatic relations with the United States. The goal of this contract is to provide the USG ships oil for them to transport to refuel the ships at sea. This is a major contract valued in the billions. The large oil company attends an industry day and identifies the acquisition and technical teams. This is an important acquisition for both the Agency and the oil company, both because of its size and because it is advertised as a departure from acquisition strategies of the past to increase competition.

The business development (BD) team of this oil company implements a multi-prong information gathering campaign to enhance its chances of winning. First, the company leverages social media to find onsite contractor employees who are badged by the Agency and have access to all of the buildings (MITRE ATT&CK, n.d.-b). They ask the contractor staff to simply pay attention to the team's meetings and locations. Next, the BD team begins to frequent local restaurant happy hours near the program lead's office building and notices that on Thursday nights, the team seems to gather at the local hotel bar (National Cyber Security Centre, n.d.). The BD team connects the gatherings to the team's all-day Thursday meetings and, over the course of a few weeks, picks up enough bits and pieces of conversation to figure out that the decision is coming down to two bidders: the incumbent and themselves. The large oil company responds to the Agency's request for Final Proposal Revisions (FPR) and decides to offset the incumbent's perceived natural advantage by eavesdropping on the team's final meeting using the location and scheduling information provided by its BD team's scouting.

The conference room's large windows and video-conferencing configuration make it a natural candidate for drone surveillance (Arthur, 2013). The BD team, who could score big bonuses and praise for their company and home country, deploys a commercial drone fixed with a camera and microphone to listen in on and observe the FPR discussion. Realizing that it is about to come in second, the BD team uses the competitive information gained to submit a last-minute "administrative correction" to its FPR pricing. Unaware of the illicit surveillance, the Agency awards the overseas fuel replenishment services contract to the state-backed oil company as the best value.

Potential impact: By monitoring the acquisition team's movements and eavesdropping on publicly held conversations loosened by the alcohol consumed in after-work gatherings, the BD

team gained situational awareness it was able to leverage to gain unfair competitive advantage in the FPR determination. If this becomes known, the Agency will be subject to public embarrassment and increased scrutiny. This has happened with large telecommunication contracts in Denmark when Huawei, a Chinese government–owned telecommunication corporation, utilized drones to spy on deliberations to win a contract (Bloomberg, 2023).

Recommendations: Agencies conducting source selections should use operational and physical security practices to ensure the integrity of the source selection remains. Additional training related to this should be included in the "just in time" training that many agencies conduct prior to source selection with the entire team.

Scenario 9: Supply Chain Risk Management (SCRM)

Acquisition Phase(s): Purchasing and Supply Chain Management

Attack/Compromise Type: Spear Phishing (Mitre, 2020)

Scenario: A foreign illegal drug cartel discovers that a company based within their country is serving as a trusted subcontractor to a USG Agency. The cartel, already adept at manipulation, compromises the trusted supplier's property management system by targeting low-level logistics clerks with spear phishing attacks that contain information about their neighborhoods.

One clerk is fooled by the spear phishing because of the specific details contained in the social media messages and clicks a spoofed link that installs rudimentary keylogging software on their work computer. Once installed, this software reports everything the clerk does back to the cartel.

The cartel uses information gathered to discover an order being processed for surveillance camera upgrades, the specifications of the ruggedized, high-resolution cameras and ordering Agency indicate they are clearly destined to monitor the border. The cartel uses its vast network and financial resources to acquire five cameras and hire software engineers to modify their firmware (MITRE ATT&CK, n.d.-e) to include "backdoors" that allow the cartel to remotely monitor and control the cameras.

Potential impact: As surveillance of the logistics clerk continues, the cartel is able to see when orders are coming in and shipments are going out. The cartel slips the counterfeit cameras into shipments going to the Prime contractor for installation. The cameras are inspected by the Prime, as well as the government, but the cameras look and operate in accordance with all of the quality assurance standards. The cartel ends up with several areas along the southern border where they can view and control the cameras doing daily surveillance.

Recommendation: Agencies with critical missions or sensitive projects should be evaluating and tracking supply chains using robust Supply Chain Risk Management (SCRM) practices. This should include requiring a detailed Bill of Materials (BOM) and Software Bill of Materials (SBOM). While these documents/files can be manipulated as well, continuously monitoring and verifying the information gives the government a view into the complex supply chains that underpin critical projects and discrepancies or vulnerabilities that have the greatest likelihood of discovery.

In this instance, an SBOM would reveal the trusted subcontractor's operation within cartel territory, and government risk managers would report this as a vulnerability to the program, knowing cartels would have a vested interest in manipulating the cameras destined for the southern border. The components from that subcontractor could be more strictly inspected, or the Vendor replaced entirely – to mitigate the risk.

Scenario 10: Banking Changes for Invoice

Acquisition Phase(s): Contract Management, Post-Award, Invoicing

Attack/Compromise Type: Spearfishing and Vendor Impersonation Fraud

Scenario: A malicious criminal seeking to score a large amount of money searches on LinkedIn for acquisition staff working in the USG Overseas Contracting Division. Gathering information from previous DoS solicitations, the actor is able to decipher the emailing convention for the USG acquisition workforce. The malicious actor poses as an industry contract administrator, emailing the USG CO in the Overseas Contracting Department stating that their banking information has changed and requesting to change it. Previous email from the industry contract administrator has come from joe.smith@industry.com. The email the CO receives this time is from joe.smith@industry..com, and they overlook the extra period at the end. The CO then sends a form to certify the change that contains their previous bank information, revealing the accurate bank information. When the CO receives an email back from the fake vendor, the payment information is updated. This new, trusted email, though it is fake, can be used to extract information such as an additional copy of the contract to include technical information, deliverables, and the Statement of Work. Once the payments are processed, the fraudulent actor is now receiving the payments, likely in very large sums. It will potentially take a few months for a business to realize that they are not receiving proper disbursements. Furthermore, the CO is likely to record that they are getting paid into the new account, which will then alert both parties that they have been a victim of fraud.

This is more likely to happen to a USG CO due to the huge variety of worldwide vendors located within and outside of the United States who support the overseas contracting division. A multitude of international vendors with different currencies and foreign languages can make for an ideal target for vendor fraud. The CO is likely to overlook subtle spelling or grammatical errors due to English not being a first language for foreign vendors.

Potential impact: A loss of federal dollars to vendor impersonation fraud will require a federal criminal and internal investigation, mitigation of data loss (e.g., bank information, any technical data, proprietary information, etc.), and significant time to recover and retrain staff. The recovery of stolen money from a bank account, the payment to the correct bank account, and the security repercussions that will be detailed in future past performance evaluations in a source selection may impact the company's financial situation and reputation.

Recommendation: Agencies that work with foreign vendors should exercise extreme caution relating to information changes and requests for documentation. Furthermore, instead of replying to new email threads, acquisition professionals should utilize previous conversations or start new ones with known email addresses. For banking changes, a formal process with confirmation by phone from vendor and a second email from a supervisor to confirm all details from industry vendor should be considered.

Recommendation

To address the unique challenges acquisition professionals face, the preceding scenarios explore common areas of improvement that can be implemented to mitigate counterintelligence risks.

To address the challenges, we aggregated all the recommendations and determined that a great deal of these risks associated with the acquisition can be mitigated at the Acquisition Strategy Phase. With this in mind, we recommend the development and implementation of an Acquisition Strategy Counterintelligence Risk Assessment (ASCRA) during the Acquisition Strategy approval process. The goal of the ASCRA is to evaluate the overall risk of conducting a

specific government acquisition in hopes of implementing mitigations early and to ensure security of the acquisition. The ASCRA would also help shape the RFP and the resulting requirements conveyed to the vendors, subcontractors, and the entire supply chain associated with each procurement. Currently, the Acquisition Strategy risk assessment conducted by nearly all Federal agencies is solely focused on the cost, schedule, and performance risks of the product or service being acquired. The repeatable ASCRA model could have broad implications across the USG and US Industrial Base, as there are currently no standardized processes for assessing the counterintelligence risk of simply conducting the acquisition. This would benefit the USG by better protecting acquisitions and benefit Industry by standardizing requirements and policies to adopt to the evolving threats rather than the current decentralized approach of acquisition operational security.

Conclusion

Acquisition vulnerabilities impact the whole of government as they create unique access points and target areas for U.S. adversaries to attack. American principles of fair opportunity and free markets require the sharing of information but also create many opportunities for foreign actors to exploit our economy. Acquisitions can unwittingly provide deep insights into the USG's most sensitive and closely guarded projects. The scenarios presented above represent possible attack vectors and are meant to be a tool to increase the acquisition community's awareness of this advancing challenge.

The proposed recommendations implementing an ASCRA in the acquisition strategy development process will enable Agencies to have a process, standard lexicon, and pre-vetted and tailorable set of mitigation strategies for any vulnerabilities that may arise during the acquisition process. Adding ASCRAs to standard Agency acquisition processes has the potential to drastically reduce the amount of U.S. resources lost every year due to adversary exfiltration and improve the overall protection of mission critical information.

Appendix A: Acronyms

AI	Artificial Intelligence
ASCRA	Acquisition Strategy Counterintelligence Risk Assessment
BD	Business Development
BOM	Bill of Materials
CO	Contracting Officer
CS	Contract Specialist
CUI	Controlled Unclassified System
FPR	Final Proposal Revisions
FTE	Full Time Equivalent
GFI	Government Furnished Information
IP	Intellectual Property
ITAR	International Traffic in Arms Regulations
NAICS	North American Industry Classification System

OT	Operational Technology
PHI	Protected Health Information
PII	Personal Identifiable Information
PM	Program Manager
RFI	Request for Information
RFP	Request for Proposal
SBOM	Software Bill of Materials
SCRM	Supply Chain Risk Management
SOW	Statement of Work
TEP	Technical Exchange Panel
USG	U.S. Government

References

Arthur, C. (2013, August 22). Laser spying: is it really practical? *The Guardian*. https://www.theguardian.com/world/2013/aug/22/gchq-warned-laser-spying-guardian-offices

Article - DDTC public portal. (2016). https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987

Bloomberg. (2023, June 19). *Huawei, Denmark and a $200 million battle over 5G*. https://www.bloomberg.com/news/videos/2023-06-19/huawei-denmark-and-a-200-million-battle-over-5g

CrowdStrike. (2023, November 6). *What is spear phishing? Definition with examples*. https://www.crowdstrike.com/cybersecurity-101/phishing/spear-phishing/

Donahue, J. (n.d.). *The top 10 social engineering tactics you need to know*. Access Systems. https://www.accesssystems.com/blog/the-top-10-social-engineering-tactics-you-need-to-know

Editor, C. C. (n.d.). *Operational technology – glossary*. CSRC. https://csrc.nist.gov/glossary/term/operational_technology

McKinsey & Company. (2023, January 19). *What is generative AI?* https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai

Mitre. (2020, March 2). *Phishing: Spearphishing link, sub-technique T1566.002 – enterprise*. MITRE ATT&CK. https://attack.mitre.org/techniques/T1566/002/

MITRE ATLAS. (n.d.-a). *Atlas.mitre.org*. Retrieved March 19, 2024, from https://atlas.mitre.org/techniques/AML.T0031/

MITRE ATLAS. (n.d.-b). *Atlas.mitre.org*. Retrieved March 19, 2024, from https://atlas.mitre.org/techniques/AML.T0043/

MITRE ATT&CK. (n.d.-a). *Audio capture, technique T1429 – mobile.* Retrieved March 19, 2024, from https://attack.mitre.org/techniques/T1429/

MITRE ATT&CK. (n.d.-b). *Gather victim identity information, technique T1589 – enterprise*. https://attack.mitre.org/techniques/T1589/

MITRE ATT&CK. (n.d.-c). *Gather victim org information, technique T1591 – enterprise.* https://attack.mitre.org/techniques/T1591/

MITRE ATT&CK. (n.d.-d). *Phishing: Spearphishing attachment, sub-technique T1566.001 – enterprise*. https://attack.mitre.org/techniques/T1566/001/

MITRE ATT&CK. (n.d.-e). *Pre-OS boot: System firmware, sub-technique T1542.001 – enterprise.* Retrieved March 19, 2024, from https://attack.mitre.org/techniques/T1542/001/

MITRE ATT&CK. (n.d.-f). *Search victim-owned websites, technique T1594 – enterprise*. https://attack.mitre.org/techniques/T1594/

MITRE ATT&CK. (2020, March 2). *Phishing, technique T1566 – enterprise*. https://attack.mitre.org/techniques/T1566/

National Cyber Security Centre. (n.d.). *Watering hole attacks*. https://www.ncsc.gov.uk/collection/supply-chain-security/watering-hole-attacks

National Institute of Standards and Technology. (2023, October 16). *NIST special publication 800-63 revision 3*. https://pages.nist.gov/800-63-3/sp800-63-3.html

Team, N. A. (n.d.). *NIST AIRC - glossary*. NIST AIRC. https://airc.nist.gov/AI_RMF_Knowledge_Base/Glossary

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net