Reveald, Inc.
31 Hudson Yards,
11th Floor
New York, NY 10001

Rob Bathurst
Chief Technology Officer

Open Letter to the Cybersecurity and Infrastructure Security Agency (CISA)

A Strategic Imperative: Transitioning from Vulnerability Management to Exploitability and Exposure Management (EEM) for Resilient Federal Cybersecurity

Dear CISA et al.,

In our current age, marked by the rapidly accelerating velocity and sophistication of cyber threats, it has become clear that traditional cybersecurity methodologies require a significant evolution. As the leaders at the forefront of national security, the urgency to not only adapt but also to proactively anticipate the evolving cyber threat landscape has never been more critical. It is within this context that I advocate for a pivotal strategic shift towards Exploitability and Exposure Management (EEM), anchored in the principles of Continuous Threat Exposure Management (CTEM). This shift promises to significantly bolster the proactive capabilities of federal agencies in preempting and countering the dynamic cyber threats of our time.

Exploitability and Exposure Management (EEM) is a strategic approach in cybersecurity that focuses on identifying and addressing the ways an attacker can enter or exploit a system (exploits) and the impact to the organization (exposures) if

REVEALD

the attack is successful. EEM goes beyond traditional vulnerability management by not only recognizing known security gaps but also anticipating potential avenues of attack that have not yet been exploited.

The goal of EEM is to proactively harden systems against both known and unknown threats, reducing the likelihood of successful cyber-attacks by managing the areas within an environment where an attack could take place. This approach intentionally decouples a threat-driven mindset focused on tactics, techniques, and procedures (TTP) and Indicators of Compromise (IOC) from organizational KPIs. This helps organizations prioritize their security efforts on the most critical areas that could be leveraged by an adversary, not ones that already have, thereby enhancing their overall security posture and resilience against cyber threats.

At this juncture, it is both pertinent and necessary to acknowledge the commendable strides already being made by the Cybersecurity and Infrastructure Security Agency (CISA) in fortifying the cybersecurity defenses of the federal government and fostering robust partnerships with the private sector. The initiatives and achievements detailed in CISA's FY2024-2026 Cybersecurity Strategic Plan lay a solid foundation upon which further advancements in our cybersecurity strategies can be built.

One of the standout achievements under CISA's stewardship has been the development and maintenance of the CISA Known Exploited Vulnerabilities (KEV) catalog. This resource represents a critical tool in the cyber defense arsenal, providing agencies and private sector partners alike with actionable intelligence on vulnerabilities that have been actively exploited by threat actors. The KEV catalog exemplifies the type of forward-thinking, proactive approach that is essential in today's cybersecurity landscape, where the speed and discretion with which threats evolve demand an equally dynamic and anticipatory response strategy.

Moreover, CISA's strategic plan articulates a clear and compelling vision for securing the cyber ecosystem against emerging threats through a combination of innovation, collaboration, and leadership. By prioritizing the reduction of systemic risk, enhancing

operational collaboration, and fostering a culture of collective defense, CISA is effectively setting the stage for a more resilient and secure digital future for all stakeholders within the national infrastructure.

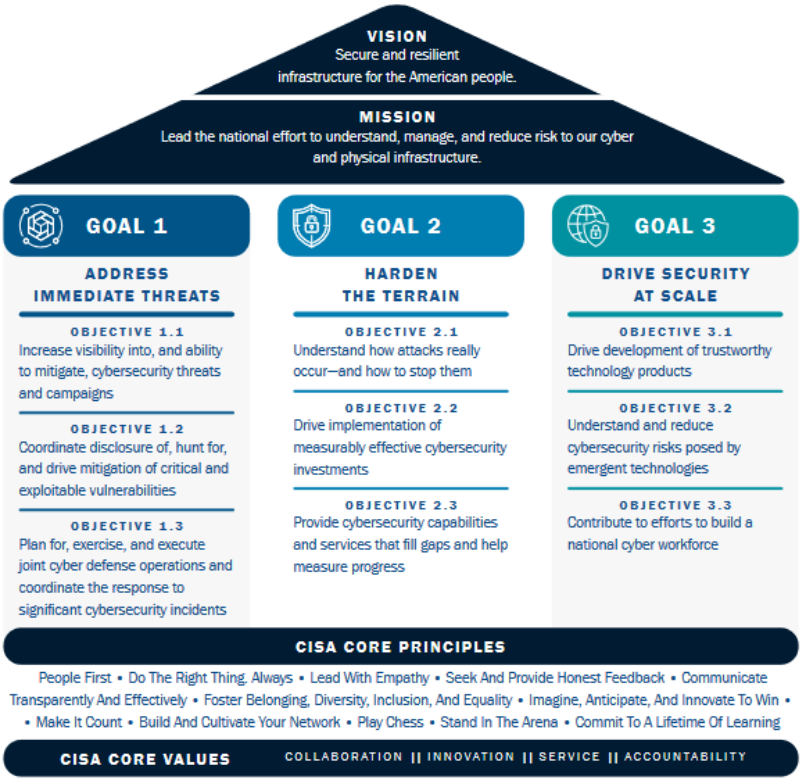

Figure 1: CISA Cybersecurity Strategic Plan Overview

EEM directly aligns with CISA's strategic goals, serving as a vital process in advancing cybersecurity on a national scale.

EEM goals:

Goal 1: EEM elevates visibility into and the capability to mitigate cybersecurity threats by preemptively identifying and addressing the avenues of potential exploitation before they manifest into immediate threats.

Goal 2: EEM embodies the essence of hardening the terrain; by pinpointing and securing the most susceptible areas within our cyber infrastructure, it aids in understanding how attacks materialize and fortifies the defenses accordingly.

Goal 3: EEM scales security measures across the board by integrating cutting-edge technologies and practices into the fabric of cybersecurity initiatives.

This alignment ensures that as new technologies emerge, their associated risks are managed effectively, contributing to the development of a resilient national cyber workforce and safeguarding our digital ecosystem against the threats of tomorrow. An EEM strategy emphasizes not just the identification and mitigation of known vulnerabilities but extends to predicting and neutralizing potential exploit paths before they can be leveraged by adversaries, especially in the face of the adversarial misuse of artificial intelligence (AI) and machine learning technologies.

Understanding the Need for Change

The landscape of cybersecurity is continuously evolving, with traditional practices centered around vulnerability and threat management increasingly proving to be fundamentally reactive. While these methods have served as the bedrock of our cybersecurity defenses, they often place us in a perpetual game of catch-up with our adversaries. The crux of the issue lies not just in the nature of the threats we face, but in the sophistication and adaptability of the actors behind them. Today, we find ourselves at a pivotal juncture where the utilization of AI by adversaries presents a profound escalation in cyber warfare capabilities.

Adversaries are looking to leverage AI to automate the discovery of vulnerabilities, orchestrate complex attacks, and mimic legitimate user behavior to evade detection. This AI-driven threat landscape enables adversaries to launch attacks at a pace and sophistication that traditional reactive cybersecurity measures cannot match. As AI technologies become more accessible, the potential for malicious use increases,

allowing attackers to exploit vulnerabilities faster than they can be patched. This rapid evolution of threats underscores the necessity of transitioning to a proactive and predictive cybersecurity model.

The integration of EEM, underpinned by the CTEM lifecycle, offers a promising pathway forward. By adopting a risk-based process that prioritizes the anticipation and preemption of potential cyber exploits, we can shift from a posture of reaction to one of prevention. EEM and CTEM enable us to identify not just the vulnerabilities but to understand and mitigate the pathways and methods adversaries are likely to use, based on real-time threat intelligence and predictive analytics. This approach not only enhances our ability to defend against known threats but also against the novel and sophisticated exploits powered by AI.

Without embracing a risk-based process, we remain anchored to a reactive stance, always a step behind in the arms race of cybersecurity. The dynamic nature of cyber threats, compounded by the adversarial use of AI, demands a transformation in our cybersecurity strategy. By prioritizing the identification of threats before they are acted upon and focusing on the most critical vulnerabilities based on their potential impact, we can establish a more resilient and adaptive defense mechanism. This strategic evolution is imperative to stay ahead of adversaries and safeguard our digital infrastructure against the next generation of cyber threats.

In-depth analysis conducted through the Epiphany Intelligence Platform (Reveald's CTEM platform that analyzes security product data to identify material risks) on over 500,000 devices demonstrates the marked advantages of an Exploit and Exposure Management (EEM) strategy— resulting in eliminating thousands of devices from critical patching consideration—over traditional vulnerability management practices. This is further underscored by Reveald’s research across eleven distinct organizations, examining 145,204 unique CVEs affecting those same 500,000 devices. It revealed that, on average, only 29% of CVEs identified by vulnerability scanners are found on systems that are deemed critical assets, and of those, a mere 4.7% present a substantial risk of exploitation. Consequently, in a typical organization

facing tens of thousands of CVEs, fewer than 2% are both exploitable and located on critical systems.

Such efficiency gains are particularly valuable considering the extensive patching requirements across major applications and operating systems within the vast ecosystem of the federal government. The resultant time savings could critically enhance the resilience of both agencies and the Defense Industrial Base (DIB) by allowing for a reallocation of efforts toward strengthening security postures.

Adopting an EEM approach does not compromise security; rather, it ensures that resources are precisely directed towards systems at genuine risk—those with potential attack exposure and technically exploitable vulnerabilities .Reveald's experience, serving a diverse clientele across key sectors such as government, healthcare, and manufacturing, demonstrates that a paradigm shift toward EEM not only conserves valuable organizational resources but also significantly bolsters the effectiveness of cybersecurity measures in preventing severe breaches.

This shift towards a risk-based cybersecurity strategy is imperative. Without it, we risk remaining perpetually reactive in the face of rapidly evolving cyber threats, including those leveraging AI for malicious purposes. By proactively identifying and addressing threats based on their potential impact, we can cultivate a more resilient and adaptable cybersecurity framework. Such a strategic evolution is crucial to outpace adversaries and protect our critical digital infrastructure from the sophisticated cyber threats of tomorrow.

The imperative for transformation is unmistakable and pressing. Adopting a risk-based cybersecurity strategy, encapsulated by EEM and CTEM, transcends being a mere alternative; it is indispensable in an era dominated by AI-enhanced threats. We are stepping into a period where the capabilities for private entities to engage in cyber warfare, either independently or as surrogates for governmental forces, are outpacing the efficacy of traditional point-solution defenses. By embracing a proactive stance in risk management and mitigation, we can forge a cybersecurity infrastructure that is

not just resilient in the face of current dangers but also nimble in responding to the evolving threats of the future.

The Strategic Advantage of EEM and the CTEM Lifecycle

- **Proactivity and Predictive Defense:** EEM, supported by CTEM's lifecycle, shifts the focus from reacting to known vulnerabilities to anticipating and mitigating potential exploit paths and exposure points focused on greatest net benefit to the organization. This paradigm enables agencies to implement defenses against threats before they manifest and know that their activities are always protecting their “crown jewels.”
- **Optimized Resource Allocation:** By identifying the most critical and likely points of exposure, EEM allows for a more strategic deployment of cybersecurity resources, ensuring that efforts are focused where they can have the greatest impact in protecting national interests. Mobilizing against exposure is about ideal resource allocation to achieve an acceptable risk result.
- **Building Resilient Systems:** The adoption of EEM within the CTEM framework fosters the development of inherently more secure systems. These systems are designed with an understanding of potential exploit vectors, making them less susceptible to attacks. The ideal environment is designed to understand that breaches will occur, but their impact can be minimal. To be resilient isn’t to be impermeable.

CTEM Lifecycle Integration for Federal Agencies and the Defense Industrial Base

Applying the CTEM lifecycle and EEM principles to a federal agency or a company within the defense industrial base can profoundly enhance national security. Through the execution of CTEM's phases—beginning with scoping the digital environment, then discovering vulnerabilities and potential attack vectors, prioritizing based on

threat impact, and validating resilience—organizations can establish a robust anticipatory defense mechanism.

When EEM is integrated, it amplifies this process by focusing on closing the most impactful exploitation opportunities and reducing exposure points, thus effectively shrinking the attack surface. Such a comprehensive approach ensures that vulnerabilities are not merely patched, but systematically managed and mitigated, significantly minimizing the risk of incidents that could jeopardize security.

By proactively addressing exposures with the insights garnered from CTEM, these organizations strengthen their resilience against sophisticated cyber threats, safeguarding critical national defense infrastructure and sensitive information integral to national security.

At its core, the CTEM model continuously cycles through these five phases:

1. **Scoping**: Establishing a comprehensive understanding of the digital terrain, including all assets and their respective importance to national security and agency operations. Scoping is an exercise in understanding what is important to the organization and why. As the first activity in the cycle, it naturally aligns security to the priorities of the agency. The needs for resilience are defined here.
2. **Discovery**: Speaking directly to the strategic goals of CISA, visibility is a core concept of the discovery phase. Using the data already present in the organization's tools and advanced analytics to uncover and assess potential exploits and exposures, beyond known vulnerabilities, to understand where organizations are most at risk. The attack paths are merely the beginning of the journey, not the end.
3. **Prioritization**: Applying impact-based prioritization to focus on securing critical assets and systems that, if compromised, could have the most significant impact on national security. The attack path tells part of the story, but the key to effective prioritization is to determine

the greatest benefit to the organization as measured by a reduction of exposure or an increase in resilience if compromised.

4. **Validation**: Validation comes in many forms. Most are familiar with how Breach and Attack Simulators (BAS) work, but validation goes beyond just the technical test. Validation is a strategy that can be broken down into four phases: Assess, Test, Measure, and Respond.
    a. **Assess**: Determine the technical viability of an attack path to achieve an objective, before determining a need to test. Saying no to a technical test is just as important as getting the results from one. Effective mobilization relies on knowing when not to deploy resources.
    b. **Test**: A technical evaluation of the attack path or condition's ability to be executed. This comes in many forms and can be conducted with many tools, but ultimately the question you're trying to answer is can the attacker go from the attack surface to the impact successfully. Regularly testing and validating the effectiveness of security measures against simulated scenarios helps measure controls and responses but needs to be focused on the impact the agency is trying to prevent.
    c. **Measure**: Determining the effectiveness of controls against known exploits and TTPs can be valuable for tuning, but it must be done with a purpose. A control is in place to counter a threat, but it should also be in place to limit exposure. By measuring the residual exposure from a potential breach, you can see the secondary and tertiary impact of exploitation. Many tools can generate events to allow measurement of controls, but very few tie the measurement back to the exposure the organization is trying to prevent.
    d. **Respond**: Testing response to validate effectiveness is the human driven aspect of this process, but conducting a purple team test just to say it's been done is a waste of resources.

Measuring effectiveness of response should be closely tied to the resilience and risk goals of the organization. Having 200 detection rules, when no one knows what you're trying to detect or prevent, isn't helpful.

5. **Mobilization**: Armed with the insights gained from these initial phases, Mobilization involves deploying rapid composite response teams with predefined tactical action plans that are informed by a comprehensive understanding of the exposures being mitigated. This phase considers the residual risk—the risk that remains after security measures have been applied—and includes contingencies for unexpected outcomes of mitigation efforts. Validation of the effectiveness of mitigation or remediation can't be overlooked. This forward-looking approach ensures that responses not only address immediate threats but also bolster the organization's defenses against future exposures.

By the time an organization reaches the Mobilization phase, it has a clear picture of its cybersecurity posture, an understanding of the adversary's tactics, and a strategic plan for immediate and decisive action.

A Call to Action

To operationalize this strategic shift, I propose:

- **Establishing a Federal Cybersecurity Innovation Task Force**: There are many task forces, commissions, and working groups in the federal government charged with evaluating tactical issues, but not many focus on practical change. This task force would be charged with developing the framework and guidelines for implementing EEM and integrating the CTEM lifecycle across federal agencies. Ideally these principles would be driven into updates of the NIST 800 standards, the CISA guidelines and directives, and align to the Executive Orders on Cybersecurity and AI. This task force directly drives the core of the National Cybersecurity Strategy's pillars to Defend Critical Infrastructure, Disrupt and Dismantle Threat Actors, and Shape Market Forces to Drive Security and Resilience.
- **Investing in Next-Generation Cybersecurity Technologies:** Allocate resources to AI and machine learning technologies that proactively predict and neutralize threats instantly. Reflecting on the successful DARPA Cyber Fast Track initiative from over 10 years ago, there's a clear need for a new, streamlined program that fosters rapid cybersecurity innovation without the burdensome federal grant application and review processes. Recognizing that most breakthroughs in cybersecurity stem from the open-source community and agile startups exploring novel ideas, the government must establish a more accessible platform to harness and integrate these advancements.
- **Launching Comprehensive Training Programs:** Cybersecurity training is challenging, even for experienced professionals. Specialization has segmented industry knowledge over the past three decades, making it rare to find experts versed in multiple domains such as offensive security, response, and operations. Rather than reflecting any shortfall in individual capabilities, this highlights the need for a broader foundational skill set. The government's training focus should be on ingraining a core understanding of essential skills and processes in cybersecurity personnel. While CTEM and EEM may not be

> flawless, they represent a crucial shift in perspective—from a tool-centric approach to one that emphasizes process and the continuous reduction of cyber exposure over merely achieving metrics.

In conclusion, the adoption of Exploitability and Exposure Management, guided by the Continuous Threat Exposure Management lifecycle, represents a forward-thinking approach to national cybersecurity. It promises not only to enhance our defensive posture but also to ensure that federal agencies remain agile and resilient in the face of an ever-changing cyber threat landscape. I urge CISA and its stakeholders to embrace this evolution with the urgency and commitment it demands, for the security and prosperity of our nation.

Sincerely,

Rob Bathurst

Rob Bathurst

Chief Technology Officer, Reveald, Inc.

March 2024