Cybersecurity and Infrastructure Security Agency (CISA)
Department of Homeland Security

Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG) General Input on the National Cyber Incident Response Plan (NCIRP) Update

Dear CISA Team,

On behalf of the Messaging, Malware, and Mobile Anti-Abuse Working Group (M³AAWG), I would like to thank you for the opportunity to provide input on the National Cyber Incident Response Plan (NCIRP) update. As a global industry organization focused on combating online abuse and improving cybersecurity, M³AAWG brings together more than 200 institutional members, including ISPs, hosting providers, email platforms, and cybersecurity experts to tackle abuse on existing networks and new emerging services through technology, collaboration, and public policy.

M³AAWG commends CISA's efforts to enhance public-private collaboration in the updated National Cyber Incident Response Plan (NCIRP). We are pleased to offer recommendations based on our extensive experience in addressing cyber threats and improving incident response. Below, we outline key areas that we believe will support and strengthen the NCIRP update. Some of these expand on aspects of the plan, while others look at issues that are not yet addressed.

1. Strengthen Public-Private Collaboration

Effective coordination between government entities and private sector organizations is essential for the prevention of cyber incidents in the first place, and for timely and efficient response when incidents occur. As the first line of defense, the private sector often detects emerging threats and possesses critical expertise that must be seamlessly integrated into federal response efforts. To achieve this, the NCIRP should provide clear guidance on the roles and responsibilities of private entities and define actionable pathways for engagement and escalation to reduce confusion and response delays. Establishing mechanisms for real-time, bidirectional information sharing—while safeguarding proprietary and sensitive data—would allow the private sector to contribute actionable threat intelligence, such as indicators of compromise and attack patterns, while benefiting from collective intelligence.

To further enhance collaboration, the NCIRP should include a dedicated incident liaison program to streamline communication and coordination during major incidents and incorporate sector-specific advisory groups to address the unique challenges of different industries, such as combating phishing

and abuse in the messaging and communication sectors. Additionally, public-private partnerships should focus on proactive measures, promoting best practices such as robust email authentication[1] and advanced anti-phishing defenses, which can reduce attack success rates. Building trust through transparency in information use and ensuring participants feel secure in contributing to these efforts are fundamental to success. By prioritizing these actions, the NCIRP can leverage the full strength of public and private capabilities for a more cohesive and effective incident response framework.

2. Enhance Abuse Reporting and Response Processes

Streamlined and effective abuse reporting is essential to addressing complex cyber threats, such as phishing attacks, malware distribution, botnet activity, and spam campaigns, which often target multiple sectors simultaneously. The NCIRP must adopt a cohesive and well-documented approach to reporting and response to mitigate these threats effectively.

M[3]AAWG recommends the inclusion of standardized reporting frameworks to ensure consistency and clarity, leveraging best practices to capture critical details like phishing email headers, malware URLs, and spam campaign samples. Establishing centralized, user-friendly reporting portals—supporting both automated submissions via APIs and anonymized submissions—will simplify the reporting process while protecting sensitive data. Furthermore, the NCIRP should implement timely feedback loops to inform reporting entities about how their data is used, actions taken, and incident status, particularly for large-scale abuse campaigns.

Integration with threat intelligence platforms is critical to ensure that abuse data, such as phishing URLs or addresses of botnet command-and-control servers, is actionable and swiftly disseminated to stakeholders like ISPs, domain registrars, and platform providers. Specific guidance should also address mitigating secondary abuse campaigns that often follow major incidents, such as coordinated takedowns of malicious domains, blocking spam, and protecting affected organizations.

The NCIRP should prioritize public awareness and accessibility by promoting education on abuse recognition. It should provide simple, widely available reporting channels, such as mobile apps or hotlines. Provisions to support resource-constrained organizations—through tools, templates, and tailored guidance—are also essential to ensuring that smaller entities can effectively participate in abuse reporting and response.

By adopting these measures, the NCIRP can strengthen the nation's capacity to identify, report, and respond to abuse campaigns. M[3]AAWG is committed to supporting the development of these processes and sharing its expertise to enhance national cyber resilience.

3. Operationalize Threat Intelligence

[1]"M[3]AAWG Email Authentication Recommended Best Practices," September 2020, https://www.m3aawg.org/sites/default/files/m3aawg-email-authentication-recommended-best-practices-09-2020.pdf

Effectively operationalizing threat intelligence is paramount to the timely identification, mitigation, and ultimately the prevention of cyber threats. In a rapidly evolving digital landscape, the ability to act swiftly on actionable intelligence can make the difference between containing an incident and allowing it to escalate. As such, the NCIRP should prioritize leveraging existing, robust threat intelligence platforms widely adopted by private-sector organizations. Many of these platforms, including those utilized by M[3]AAWG members, provide valuable insights into the latest threat trends, attack vectors, and evolving tactics employed by malicious actors.

By integrating private-sector threat intelligence into the NCIRP, federal agencies gain access to a wealth of critical data. This includes indicators of compromise (IOCs), attack vectors, and behavioral patterns that have been observed in real-world situations. Such intelligence is invaluable for identifying threats early, facilitating rapid mitigation, and enhancing situational awareness at both the national and organizational levels. This collaboration between the public and private sectors can enable federal agencies to act more swiftly and effectively, while simultaneously equipping private-sector entities with the intelligence needed to fortify their defenses before incidents spiral out of control.

Additionally, it is essential to foster a seamless, bidirectional exchange of threat intelligence. This exchange allows private-sector organizations to contribute insights on emerging threats, such as new malware variants, phishing campaigns, and zero-day vulnerabilities, while simultaneously receiving timely updates on federal actions or alerts. This collaborative flow of information ensures that both the public and private sectors remain aligned in their response strategies and are positioned to identify and disrupt malicious activities quickly before they can cause widespread harm. By establishing provisions in the NCIRP for operationalizing these efforts, the U.S. can bridge existing intelligence gaps, enhance national cybersecurity resilience, and strengthen protections across shared digital ecosystems.

Operationalizing threat intelligence through these mechanisms would also allow for more proactive threat-hunting and vulnerability management, significantly reducing the time between identifying and containing malicious activities. Furthermore, the consistent exchange of threat intelligence strengthens relationships between sectors and contributes to a culture of mutual trust and collaboration critical for the evolving cyber threat landscape.

Incorporating these provisions into the NCIRP would not only accelerate the response to cyber incidents but also serve as a force multiplier, increasing the overall effectiveness of both public and private cybersecurity efforts. It would ensure a comprehensive, coordinated, and data-driven approach to mitigating cyber risks at scale.

4. **Address Messaging Abuse**

Messaging platforms, including email, SMS, and other communication channels, are essential to everyday communication and remain critical vectors for cyber incidents. These platforms are frequently exploited for phishing attacks, Business Email Compromise (BEC), malware delivery, and

other forms of cyber abuse. As such, the NCIRP must explicitly recognize these communication channels as high-risk attack surfaces and integrate targeted measures designed to mitigate abuse during and after a cyber incident.

Phishing attacks continue to be among the most prevalent threats, with cybercriminals often relying on deceptive email or SMS messages to trick individuals into revealing sensitive information. BEC attacks in particular have resulted in significant financial losses for organizations by impersonating trusted executives or partners. To combat these threats, the NCIRP should advocate for the implementation of standardized authentication protocols such as DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting, and Conformance) for email. These protocols, when properly configured and adopted across organizations, can significantly reduce the impact of email-based attacks by ensuring the authenticity of the sender's domain name and detecting unauthorized domain-name spoofing.

Beyond email, SMS-based phishing (also known as "smishing") and abuse of messaging platforms for spam and other malicious activities are growing concerns. To address these, the NCIRP should promote the adoption of anti-spam and anti-abuse frameworks specifically designed for SMS, messaging apps, and other communication platforms. By deploying real-time filtering, threat detection, and automated response mechanisms, stakeholders can identify and mitigate malicious campaigns before they spread further. This includes leveraging tools based on machine learning for spam detection and then integrating them with existing messaging systems to block known malicious sources automatically.

Given the widespread reliance on messaging for both business and personal communication, ensuring the security and integrity of these channels during cyber incidents is paramount. Attacks targeting these platforms can quickly escalate, affecting not only the targeted individuals or organizations but also their clients, partners, and customers. By prioritizing the security of messaging systems in the NCIRP, the federal government, private-sector organizations, and service providers can work together against these threats by improving mechanisms for reporting abuse, enhancing user education on recognizing suspicious messages, and coordinating rapid responses to incidents involving large-scale messaging abuse.

Furthermore, due to the interconnected nature of messaging systems across various sectors, M^3AAWG urges the NCIRP to develop and clearly define protocols for effective coordination among telecom providers, email service providers, platform owners, and other stakeholders during large-scale incidents. This collaboration will allow for swift takedowns of fraudulent accounts, blocking of malicious domains, and disruption of coordinated attack campaigns across multiple platforms simultaneously.

Incorporating comprehensive measures to address messaging abuse within the NCIRP will enhance the nation's ability to protect users from emerging threats and ensure that attackers cannot exploit these vital communication channels to escalate their attacks. By integrating the protocols and frameworks noted above into the incident response process, both federal and private-sector

stakeholders can respond more effectively to messaging-based threats, preventing attackers from exploiting these critical systems to further their malicious objectives.

5. **Educate Stakeholders**

Training and preparedness are critical components of a robust cyber incident response framework. The ability to effectively respond to coordinated cyber incidents requires not only the appropriate technology and processes but also a well-prepared workforce. For this reason, the NCIRP must prioritize the development and implementation of comprehensive training programs and exercises to ensure that both public and private sector actors possess the necessary knowledge, skills, and coordination capabilities to respond swiftly and effectively to cyber incidents.

Effective training should cover all stages of an incident, from early detection and assessment to response, recovery, and post-incident analysis. These programs should include scenario-based exercises that replicate real-world incidents, enabling stakeholders to practice their roles in a simulated, high-pressure environment. By doing so, participants can gain hands-on experience in handling cyber threats and refining their response strategies before an actual incident occurs. This will also allow organizations to identify gaps in their processes, communication channels, and decision-making procedures, and to make adjustments before a real crisis arises.

Leveraging existing resources and best practices from trusted entities like M^{3}AAWG can provide a solid foundation for these educational initiatives. M^{3}AAWG's extensive expertise in abuse mitigation, threat intelligence sharing, and incident response can offer valuable insights into tackling the complex challenges of modern cyber incidents. Through M^{3}AAWG's resources, stakeholders can gain knowledge on the latest trends in cybercrime, emerging threat vectors, and how to integrate threat intelligence into their day-to-day operations. M^{3}AAWG's Best Practices documents,[2] based on years of practical experience, can help ensure that all parties are aligned not only in their incident response capabilities but also in their overall approach to cybersecurity.

Training should also emphasize collaboration and communication between federal agencies, private-sector organizations, and other stakeholders. Effective coordination among different entities during an incident can make the difference between rapid containment and widespread damage. The NCIRP should include provisions for cross-sector training that fosters relationships and trust among government agencies, industry groups, and private companies. Such training will also prepare stakeholders to navigate the complexities of legal, regulatory, and compliance issues that may arise during an incident, ensuring a swift and legally compliant response.

In addition to formal training programs, the NCIRP should encourage continuous learning and knowledge sharing. The rapidly evolving nature of cyber threats means that stakeholders need to stay updated on new attack methods, tools, and defensive technologies. A culture of continuous learning, supported by ongoing access to up-to-date resources, research, and expert advice, will ensure that

[2]See the full list of M^{3}AAWG's Best Practices at https://www.m3aawg.org/published-documents

stakeholders remain agile and capable of adapting to emerging threats. The NCIRP should facilitate the creation of a learning ecosystem, where stakeholders can access webinars, workshops, and conferences, as well as engage in peer-to-peer collaboration and information sharing.

Finally, education should extend beyond traditional stakeholders to include smaller organizations and the general public. Many organizations, particularly small and medium-sized enterprises, may lack the resources to implement robust incident response plans. Providing targeted education and training to these groups can help them understand basic cybersecurity principles, the importance of reporting incidents, and how to access support when needed. Similarly, public awareness campaigns can help individuals recognize common threats such as phishing and identity theft and take appropriate actions to safeguard their personal information.

By investing in training, preparedness, and education at every level, the NCIRP can ensure that federal and private-sector organizations are not only equipped to respond to cyber incidents but are also empowered to prevent them from occurring in the first place. By fostering a culture of continuous learning, collaboration, and proactive threat mitigation, the NCIRP will build a resilient cyber ecosystem where stakeholders work together to prevent, detect, and respond to threats effectively, minimizing the potential damage from cyber incidents.

6. **Incorporate Abuse Mitigation into Incident Planning**

As cyber threats continue to evolve, it is crucial that the National Cyber Incident Response Plan (NCIRP) incorporate strategies for abuse mitigation as a core component of its incident response framework. Cyber incidents often trigger not only direct attacks but also secondary abuse activities such as spam campaigns, credential stuffing, phishing, and other forms of malicious activity that exploit the chaos of a larger event. These secondary threats can compound the damage from an initial breach, often escalating the severity of the incident and extending the duration of the response. Therefore, it is imperative that the NCIRP prioritize abuse mitigation as part of its comprehensive incident response planning.

A key aspect of effectively addressing abuse during a cyber incident is the ability to quickly identify and respond to these malicious activities in real time. For instance, credential stuffing attacks—where attackers attempt to exploit previously stolen credentials—often accompany larger data breaches. Similarly, spam campaigns and phishing attempts can increase dramatically in the aftermath of a security incident as attackers attempt to capitalize on the confusion and panic. With strategies for detecting and preventing these forms of abuse integrated into the NCIRP, response teams can more effectively mitigate their impact, reducing the window of vulnerability and limiting further harm to individuals, organizations, and the wider digital ecosystem.

The NCIRP should include clear, actionable strategies for identifying key abuse indicators such as abnormal traffic patterns, suspicious authentication attempts, and the proliferation of fraudulent communications. These strategies should emphasize the rapid identification of malicious domains, IP addresses, and other critical attack vectors that facilitate abuse activities. In doing so, the NCIRP

will enable stakeholders to proactively address secondary attacks, limiting their ability to disrupt operations and undermine public confidence in response efforts.

M[3]AAWG's established frameworks and best practices, honed over years of experience combating messaging abuse and related threats, provide a robust foundation for supporting the NCIRP's abuse mitigation strategy. M[3]AAWG's work in creating standardized protocols for abuse reporting, including the identification of IOCs related to phishing, spam, and other messaging-based threats, is particularly valuable. M[3]AAWG's abuse mitigation guidelines and incident response recommendations can help inform best practices for addressing abuse in real time.

Additionally, M[3]AAWG's focus on collaboration between public and private sector stakeholders offers valuable insights into coordinating efforts during an incident. Effective abuse mitigation requires seamless information sharing and coordination across various entities, from ISPs and domain registrars to government agencies and private-sector companies. The NCIRP should ensure that mechanisms are in place to facilitate this collaboration, ensuring that abuse data is rapidly disseminated and that mitigation actions can be taken in a coordinated manner.

One key aspect of this collaboration is the integration of automated tools and threat intelligence platforms that can enhance real-time detection and response. By leveraging M[3]AAWG's frameworks, the NCIRP can promote the use of automated detection systems for identifying spam campaigns, credential stuffing attempts, and other forms of abuse. These tools can provide immediate alerts and enable rapid remediation, reducing the time it takes to neutralize threats and minimize their impact.

Moreover, the NCIRP should include provisions for post-incident review and continuous improvement. After a cyber incident, a thorough evaluation of the effectiveness of abuse mitigation strategies should be conducted, with a focus on identifying lessons learned and refining response procedures. This feedback loop will help to strengthen the NCIRP over time and ensure that it remains adaptable to new and emerging forms of abuse.

With abuse mitigation strategies integrated into the core incident response planning of the NCIRP, stakeholders will be better equipped to handle the complexities of modern cyber threats. The proactive identification and disruption of secondary abuse activities, coupled with M[3]AAWG's established frameworks and real-time coordination efforts, will ensure a more comprehensive and effective response to cyber incidents. This approach will help to protect the integrity of communication channels, maintain public trust, and minimize the broader societal impact of cyber threats.

7. **Ensure a Scalable and Predictable Framework**

The NCIRP must incorporate scalable processes that can adapt to the evolving nature of cyber incidents, recognizing that attacks like Distributed Denial of Service (DDoS) often start small but can escalate rapidly. Having scalable response capabilities in place will be essential to managing the

increased impact as these incidents develop. The ability to allocate resources, share real-time data, and respond flexibly is key to mitigating the broader effects of a growing cyber threat.

Equally critical is ensuring predictability and consistency in the government's response, which plays a vital role in fostering trust within the private sector. When businesses know what to expect and can rely on clear, established protocols for engagement, collaboration can occur faster and with greater efficiency. Reducing uncertainty during high-pressure incidents is crucial for minimizing delays and preventing unnecessary complications that can amplify the impact of the attack.

To achieve this, the NCIRP should focus on creating clear communication frameworks and standardized procedures for escalating incidents based on their severity. A reliable classification system for incidents, along with predefined roles and responsibilities for response teams, will ensure that the response is both efficient and effective, allowing for a swift recovery. By integrating automated tools and maintaining a continuous evaluation process, the NCIRP can ensure that its response capabilities remain flexible, responsive, and efficient as incidents unfold.

A scalable and predictable framework will not only enhance the coordination between the public and private sectors but also ensure that cyber incidents are addressed swiftly and effectively. This approach strengthens the overall resilience of the nation's digital infrastructure and fosters long-term trust, ultimately improving the collective cybersecurity posture and enabling quicker recovery from cyber threats.

8. **Focus on the Global Dimension**

In today's interconnected digital landscape, cyber incidents frequently have international ramifications, especially when they involve cross-border abuse or threat actors. The NCIRP must recognize that cyber threats do not respect national borders, making it critical to account for the global dimension of incidents. These incidents often transcend geographical boundaries, affecting organizations and individuals across multiple countries simultaneously. As a result, coordinated international responses are essential to mitigate the broader impact of such incidents.

To address this, the NCIRP should integrate global best practices that promote cross-border collaboration. By aligning with international frameworks and standards such as those developed by M^3AAWG and other global cyber threat organizations, the U.S. can help ensure a unified and effective approach to addressing cyber threats. M^3AAWG's international approach to combating messaging abuse, phishing, spam, and other cyber threats offers proven strategies that can be leveraged globally to tackle cyber incidents more comprehensively.

Moreover, by incorporating these global best practices, the NCIRP can strengthen international partnerships, making it easier to share threat intelligence and coordinate responses across borders. This not only enhances the U.S. government's ability to respond to cyber threats but also bolsters global cybersecurity resilience. A collaborative approach that incorporates international expertise and resources will ultimately lead to more effective mitigation efforts and contribute to the development

of a more secure global digital ecosystem. Such collaboration is also key to an important early step in this process: prevention of incidents in the first place by leveraging shared information, collaborative law enforcement, and deploying technologies such as multi-factor authentication,[3] with a goal of keeping bad actors out from the start.

9. **Incorporate AI and Emerging Threats**

As technology rapidly evolves, so do the threats that accompany it. Artificial Intelligence (AI) has begun to play a significant part on both sides, and its role will continue to grow. On the one side, AI is itself a threat vector, while on the other, AI-based threat detection and mitigation can be a very powerful tool.

One of the most pressing concerns for the NCIRP is the emerging risk posed by AI-driven threats, including sophisticated attacks such as deep fake phishing, automated spam, and other forms of AI-generated abuse. These threats represent a new frontier in cybersecurity as they leverage advanced technologies to bypass traditional defense mechanisms and deceive both individuals and organizations on an unprecedented scale. Addressing these emerging risks requires forward-thinking strategies that consider the growing role of artificial intelligence in cyber threats.

To adequately prepare for and respond to these threats, the NCIRP should prioritize guidance on the use of AI and machine learning technologies to detect, identify, and mitigate abuse in real time. AI can play a crucial role in identifying patterns and anomalies in large datasets, enabling quicker detection of threats such as deepfake phishing, where attackers use AI-generated images or videos to impersonate trusted individuals or organizations. Similarly, AI can be leveraged to counter automated spam campaigns that flood inboxes, evading traditional spam filters through increasingly sophisticated tactics.

By incorporating AI and machine learning into threat detection and response, the NCIRP can enhance the speed and accuracy of incident identification, allowing for faster mitigation of emerging threats. Additionally, AI-driven technologies can be used to automate the detection of suspicious behaviors and patterns, providing real-time insights that empower both public and private sector entities to take immediate action.

Ultimately, integrating AI into the NCIRP will ensure that the response framework remains adaptable and effective in the face of rapidly evolving cyber threats. This proactive approach will better equip organizations to handle emerging risks while safeguarding against the next generation of AI-driven cyber threats.

We hope our feedback provides practical insights to help strengthen the NCIRP's focus on preventing and mitigating abuse, fostering collaboration, and improving the overall effectiveness of the nation's cyber incident response efforts.

[3] "M[3]AAWG Multifactor Authentication Recommendations," February 2017, https://www.m3aawg.org/sites/default/files/m3aawg-multifactor-authenication-bp-2017-02.pdf

We appreciate the opportunity to submit feedback and welcome further engagement as needed to answer any questions during this process. Please address any inquiries to M[3]AAWG Executive Director Amy Cadagin at comments@m3aawg.org.

Sincerely,
Amy Cadagin
Executive Director
Messaging Malware Mobile Anti-Abuse Working Group (M[3]AAWG)
comments@m3aawg.org
P.O. Box 9125, Brea, CA 92822