Before the

National Telecommunications and Information Administration, Department of Commerce

Washington, DC 20230

In the Matter of	)	
	)	
Introduction of Accountable	)	Docket Number: 230412-0099
Measures Regarding Access to	)	/ NTIA–2023–0006
Personal Information of .us	)	
Registrants	)	

Comments of the Messaging Malware Mobile Anti-Abuse Working Group (M³AAWG) on the Introduction of Accountable Measures Regarding Access to Personal Information of .us Registrants

Introduction and Context

The Messaging Malware Mobile Anti-Abuse Working Group (M³AAWG) appreciates the opportunity to submit comments in response to the Agency's request. M³AAWG is a technology-neutral global industry association. As a working body, we focus on operational issues of internet abuse including technology, industry collaboration, and public policy. With more than 200 institutional members worldwide, we bring together stakeholders in the online community in a confidential yet open forum, developing best practices and cooperative approaches for fighting online abuse.

Executive Summary

While M³AAWG understands and sympathizes with some of the legitimate concerns driving this proposed policy change, M³AAWG supports access to WHOIS data to the maximum extent possible to meet all legally permitted aims, including end users' legitimate interests in avoiding spam, scams, abuse, and phishing as necessary and proportionate. In the absence of clear federal privacy legislation and in light of the importance of functional WHOIS for anti-abuse actors and end users, M³AAWG strongly supports unlimited, unencumbered access to .us WHOIS at this point and believes that more detail is needed to assess any proposal for change.

M³AAWG concludes that the currently described solution is likely to produce unintended consequences that could make the .us registry subject to more abuse (as described in more detail below) resulting from the loss of transparency. Less intrusive measures are available to avoid these unintended consequences.

M³AAWG also requests that the Agency publish additional data supporting the nature and extent of the problems seen with today's system as well as the rationale for proposing the email delivery system. Understanding the motivation for the change and the nature of the problem will lead to a better solution – a solution that has a reasonable expectation to solve the problem that the Agency is trying to address. If the Agency chooses to change current processes, we hope that the Agency will conduct a full Privacy and Security Impact Assessment of the changes and arrange multiple, more detailed public comment periods to address any implementation challenges.

In summary, M³AAWG urges the Agency NOT to implement the potential changes described in this request for comments. In the event the .us WHOIS access policy is changed, M³AAWG encourages the Agency to ensure full public access to information about legal persons (which by their nature do not have privacy rights), and to continue to provide access through the existing WHOIS scheme – preferably through the more modern and flexible Registration Data Access Protocol (RDAP). Providing access via email is ill-advised because it would be unreliable, insecure, and incompatible with every other WHOIS provider. If the data of natural persons is to be redacted, M³AAWG recommends the use of hashing rather than blanket removal and the creation of a full access scheme for both private and government anti-abuse actors.

Finally, M³AAWG notes that the accountability sought by the Agency focuses exclusively on the requester of the data and does not address the accuracy of data received from the registrant. M³AAWG encourages the Agency to consider verification rules from the registrant to minimize the amount of abuse in the .us registry.

Section I addresses specific questions from the RFC. Section II addresses specific elements included in the Proposed Scheme.

Section I. Specific Questions from the Agency RFC

1. In general, what are your views on the public availability of the usTLD domain name registration data to anonymous users? […] And, whether or not you are aware of examples of such abuse, do you believe that there is a significant risk of such abuse occurring in the future, if the current system remains unchanged (and if so, why)?

Based on our data and experience, most of the risk .us faces comes not from harvesting of WHOIS data, but from inadvertently creating conditions that enable abuse of .us domains for phishing, spam, scams and other online abuse and criminality. The availability of full .us domain registration data has positive impacts on domain abuse involving .us domains, as abusers tend to avoid public scrutiny enabled by data access. This "open source" model of policing has prevented .us from becoming known as a hotbed of abuse, as some other registries have.[1] Having an open WHOIS that allows attribution leads to proactive mitigation efforts that stop abuse before it happens. We suggest that the Agency refer to the APWG and M³AAWG

[1] Contrast .us with other TLDs listed at, for example, https://www.spamhaus.org/statistics/tlds/

reports[2] on the impact of redactions of the WHOIS by other registries, as well as the reports by Interisle Consulting.[3] Furthermore, having available registration data allows third parties to audit/verify that .us nexus requirements are being met.

2. Do you believe the current system of anonymous access to usTLD domain name registration data should remain unchanged? If so, why?

Yes, we would recommend leaving it unchanged if the system proposed by the Agency is not designed to accommodate the needs of cybersecurity investigators for real-time, high-volume access. It currently works and works well, and consumers who may not agree with the current policy always have the option to purchase and use domains from some other TLD that better aligns with their preferences. At the moment, the proposal laid out is not detailed enough to provide a full assessment technically and procedurally. Please refer to the 2021 M[3]AAWG WHOIS study, which explains the problems experienced by M[3]AAWG members arising out of the lack of WHOIS availability in gTLDs since 2018.[4]

Before adopting any proposal or deciding to change the current approach, M[3]AAWG recommends that the Agency conduct a study to ascertain the level of abuse associated with an open WHOIS system, and a corresponding study from users of WHOIS to identify the harms that would be caused if the open WHOIS system were no longer available. A Privacy and Security Impact Assessment should be commissioned before any change in personal data processing is put into effect. Part of that process would be engaging with all stakeholders to properly balance the rights of all parties and would allow for a formal recognition of the rights-protecting impact of the current access model. Any such balancing would require study to ascertain the level of abuse associated with an open WHOIS system. We recommend that the agency reevaluate the system once it has carefully examined the results of these studies and established that the proposal's features will meet the goals for the change.

3. What legitimate purposes for access to usTLD domain name registration data should be included in the System's pre-defined list? Please provide a rationale for each category recommended.

We question the effectiveness of the proposed approach. Without proper audit and enforcement (which is unachievable with the proposed email solution, as it does not provide actual authentication or identity verification), selecting a use case would in practice be moot.

Nevertheless, if a categorization is to be adopted, we would suggest (in alphabetical order):

- Academic research
- Anti-fraud/anti-malware/anti-phishing/anti-spam
- Brand protection
- Commercial uses other than marketing (such as supporting litigation)

---

[2] "ICANN, GDPR and WHOIS Users Survey" http://www.m3aawg.org/WhoisSurvey2018-10 and "ICANN, GDPR, and the WHOIS: A Users Survey - Three Years Later" https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

[3] "WHOIS Contact Data Availability and Registrant Classification Study: A Study of the Effects of GDPR and ICANN Policy," https://www.interisle.net/ContactStudy2021.pdf

[4] "ICANN, GDPR, and the WHOIS: A Users Survey - Three Years Later," https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

- Consumer protection (consumers identifying and confirming the businesses they do business with)
- Copyright infringement investigations (pirated books and periodicals, games, movies, music, software, etc.)
- Due diligence for corporate merger/acquisition
- Domain sales and acquisitions (e.g., validating a user really is the owner of a domain they claim to be selling)
- Financial institution KYC (Know Your Customer) due diligence
- Law enforcement/national security (including anti-terrorism investigations)
- Online child sexual abuse material (CSAM)-related investigations
- Operational networking and system-related issue resolution
- Risk management
- SSL/TLS certificate request due diligence
- Trademark infringement investigations (knock-off merchandise such as clothes, jewelry, shoes, watches)

We further believe that the .us policy should clearly list the specific purposes that are not allowed, rather than place the burden on the requester to justify any new purposes through the use of a free-form text to be manually reviewed by the .us contractor.

In our view, the denials should be limited to a few identified categories, such as "marketing," "spam," "data harvesting," and "abuse."

4. Are there policies and practices developed or employed by other ccTLDs regarding WHOIS access that could be incorporated into the usTLD space? Please be specific in your response.

We encourage the Agency to look beyond other ccTLDs to IP WHOIS. Unlike domain WHOIS, IP WHOIS remains largely intact and useful, with real information about resource holders. In our opinion, IP WHOIS is the model .us should follow.

The practices of ccTLDs may be instructive with regard to the *comprehensive* treatment of WHOIS, including the accuracy or verification of registrants, which often results in reduced levels of abuse. For example, the .dk ccTLD has WHOIS requirements that include making certain contact data fields public. Having a more accurate WHOIS in the .us registry should reduce the need to access WHOIS since the abuse levels should be reduced.

5. Should the System distinguish between personal and non-personal registration data, and if so, how?

We assume this question is focused on whether domain registration data from the registrant should be treated differently depending on whether the data reflects the data of a natural person or that of a legal person.

In general, we urge you to consider continuing the current transparent model of sharing all registrant data until such time as the US adopts federal privacy legislation. At the same time, we note that legal persons like corporate entities are not protected by privacy laws; only humans are. Therefore, there is no reason to redact

or encumber access to non-personal data, and there are compelling reasons for legal persons to publish such data related to domains they control.

6. Should usTLD registrants be notified when their data is accessed through the System? If so, why, when or in what circumstances?

In the event that the proposal is adopted, law enforcement access should be subject to a "gag order" precluding notification, since notification may jeopardize the investigation and cause cyber-flight. Furthermore, requests related to anti-abuse from cybersecurity professionals would also benefit from not being followed by an immediate notification for the same reason.

We note that several different notification models are potentially applicable, but it is unclear how they would be useful. Sharing statistics with domain registrants as a general informative measure – potentially as a summary report – might be informative but will not be actionable. Giving more data does not really change the fact that actionability remains minimal, unless .us were to communicate the contact details of the requester, which comes with its own drawbacks and concerns. However, as we outlined, the use of email aliases makes this approach moot.

The correct context for this question to be considered is a complete Privacy and Security Impact Assessment, which would allow for competing interests to be considered, and a conscious balancing between them to be struck.

7. Under what circumstances, if any, should the Contractor require certain requesters to furnish a warrant when requesting access to usTLD registration data?

While we argue against redacting the WHOIS for .us, warrants might be required for requesting information beyond the standard WHOIS fields, such as payment information. However, we would assume that such instances are relatively rare for the .us registry considering its role in the DNS ecosystem.[5]

8. The Contractor has proposed that the System provide special access to recognized and authenticated law enforcement and similar entities. Please provide feedback on this concept. If this proposal is adopted, how should it work? Are there best practices in other similar situations or other TLDs that could be used for such a special access portal? What steps should be taken, if any, to ensure the confidentiality of law enforcement requests through the System?

There appears to be an assumption that law enforcement officers (LEOs) are the only ones working to combat internet abuse. The overwhelming majority of anti-abuse activity is conducted and managed by non-LEOs, including ISPs, commercial security companies, private individuals, academics, and journalists, who constantly work on combating internet abuse. Limiting access to LEOs only will undercut many of those collaborations and increase abuse of .us domains.[6]

[5] Such data would be available at registrar level.
[6] See "ICANN, GDPR, and the WHOIS: A Users Survey - Three Years Later," https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

We also note that the status of LEOs is not as clear-cut as it might seem. Various US and international agencies, tribal investigators, and public-private partnerships run investigations but are not always sworn law enforcement officers.[7]

Last but not least, many LEOs have indicated that they cannot use data they have "special access" to in preliminary investigations for due process and other policy issues. The creation of a "special access" for LEOs may turn out in fact to make investigations of crime, abuse, and so on more difficult not only for non-LEOs, but also for LEOs.

As to ensuring the confidentiality of law enforcement requests, ultimately law enforcement would likely prefer to be able to download comprehensive WHOIS data for access and analysis on their own systems. Any less discrete access will be prone to query monitoring and mining, potentially compromising sensitive investigations.

9. What entities in addition to law enforcement, if any, should have special access to usTLD registration data through an authenticated portal? Why?

First, we note that overwhelmingly, anti-abuse activity on the internet is conducted by private parties, sometimes, but not always, in direct cooperation with law enforcement. For a variety of reasons that include the technical nature and architecture of the internet infrastructure, law enforcement is not able to take over these efforts.

Second, we note that anti-abuse actors, both law enforcement and private, are constantly requesting and reacting to data to prevent and respond to ongoing abuse. For this use case, domain-by-domain requests are unlikely to be workable. Thus, API access is necessary.

Beyond sworn law enforcement, including but not limited to federal agents, state police, local police, sheriffs, and tribal law enforcement officers, many civil investigators also have a need for access to .us WHOIS data. Examples of this would include Federal Trade Commision (FTC) investigators, state attorneys general, and similar civil enforcement officers. The Agency must ensure that they create and clarify a full list of relevant parties, including such civil agencies and non-government actors.

The Agency may also want to give special consideration to international law enforcement agencies, how they should be treated, and which of those (if any) should be treated as equivalent to US law enforcement agencies for access purposes.

Beyond that, the line between "law enforcement," the intelligence community, and the military may also be blurry at times.

10. What accountability and/or enforcement mechanisms should be put in place in the case of breach of the System's TOS by those that access the registration data?

Given the effective pseudo-anonymity of email-based identifiers, and the reality that if one email identifier is blocked, another can readily replace it, *effective* action against terms of service violators is difficult at best, if not practically impossible at scale.

[7] See our response to question 9 for more details.

More stringent identity proofing, posting of a financial bond, or linkage of an email address to a second identifier or a tangible identifier might ameliorate this issue. However, we believe that measures employed should be never more than is strictly necessary and proportionate to the purposes they are intended to serve and commensurate with the risks involved. The traditional WHOIS public model has been in place for many years, and it appears that negative impacts have not been particularly severe.

11. Do you foresee any challenges to implementation of the System, or elements thereof, for example in distinguishing between personal and non-personal registration data, enforcement of System misuse, etc? If so, how might these challenges be addressed?

We have addressed many challenges elsewhere in this document, and we note that some inconsistencies are present; for example, the system is described as providing immediate, automated response for most requests but still asks questions about special access and accelerated access that would only be necessary if the system were not to respond as described. The "WHOIS via email" model is simply too error-prone. It is not suitable for exchanging structured data and should be abandoned.

12. Should the Accountable WHOIS Gateway System be offered as an opt-in or opt-out service for current and new usTLD domain name registrants?

We maintain that redacting contact details will adversely impact the value and usability of already registered .us domains. These domains have historically been valuable and trusted in part because they have traditionally been more transparent than competing domains. Since registrants intending to use their .us domain name for abuse will have no incentive to opt in to the publication or disclosure of their data, we believe an opt-in model is ill advised.

Section II. Concerns About the Elements Included in the Proposal

(Element 1) The System would require those seeking access to the usTLD registration data to provide their name, an email address, and to accept the Terms of Service (TOS). The TOS would require the user to agree not to misuse the data.

M[3]AAWG appreciates the desire to create accountability with the disclosure of WHOIS data. However, the requirement to provide an email address will not produce accountability for misusers, since there is no accompanying verification of the requester. An email address alone does not serve as an identifier of the requesting party. Moreover, an email address is not necessary to achieve acceptance and enforcement of the Terms of Service, since the TOS can be included in the portal, website, or included with the data delivered in response to the query. Thus, the result of this proposal would be the perverse outcome of holding good faith actors to account and slowing down their requests, while allowing bad actors to process registration data without fear of negative consequence since bad actors ignore the TOS.

(Element 2) Users would also be required to identify, from a pre-selected list, a legitimate, non-marketing purpose for accessing the information. This list would be developed according to industry best practice in consultation with the usTLD community and approved by NTIA.

M[3]AAWG notes that there are many legitimate, non-marketing purposes for accessing the information, and that a pre-selected list may not be inclusive enough to address the legitimate purposes allowable under US

law. There is also a concern regarding the reference to industry best practices. It is the experience of M[3]AAWG members that gTLD registrars and registries have been restricting access to WHOIS information since 2018 in a manner that is overly restrictive and beyond what is necessary to comply with applicable privacy laws.[8]

A user-provided name and email address does not equate to any sort of persistent identity. Email addresses are simple to create and usually free. Malicious parties will likely create and exploit as many disposable email accounts as necessary to defeat the proposed new scheme.

Thus, requiring the accessing party to "accept the Terms of Service" and "agree not to misuse the data" would likely be without effect. Unless the agency proposes to engage in expensive litigation to investigate and enforce breaches of their ToS, bad actors will know that they can freely accept the ToS and misuse the acquired data as they please.

Further, it is unrealistic to expect that an abusive user can be trusted to self-assert their actual intended use for the data. Instead, M[3]AAWG encourages the Agency to consider other more effective methods of identifying abusers, such as to establish "honey pots" – domain names registered to bait bad actors into sending spam, phishing, or other malicious registrations.

(Element 3) Unredacted WHOIS data would then automatically be returned in near-real-time to the user via email.

We note that the proposed email delivery mechanism is not defined in the proposal, making its assessment difficult.

First of all, we could not determine how WHOIS data would be formatted and transmitted. For example:

- Would data be plain text only, or would there be attachments?
- What character set will be used – UTF-8, or something more universal?
- Will the attachments, if any, be text-based, or perhaps consist of PDFs?

It is also unclear how bulk requests would be possible and how they would be treated and responded to. Clearly, the usability and effectiveness of the proposed system would vary depending on the answers to these questions.

Technically, email represents a poor medium for the exchange of structured data such as WHOIS information. Tried and tested solutions such as the RDAP protocol exist and represent a better approach. In comparison, using email comes with major drawbacks:

- **Email delivery of WHOIS is unreliable.**

  Email may get filtered – particularly emails containing known suspicious or malicious domain names. A considerable number of the domains being queried likely relate to spam, phishing, scams, the distribution of malware, or other abusive online behaviors. Spam filters will delete or junk email

[8] See "ICANN, GDPR, and the WHOIS: A Users Survey - Three Years Later," https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

messages containing references to those domains, making it impossible or at least cumbersome to receive these data. Thus, cybersecurity investigators may not receive the data at all or may not receive it in a timely manner. Without a direct connection such as RDAP, it might be difficult or even impossible to find, diagnose, and fix delivery issues.

- **Email can be easily spoofed.**

  The use of email security and anti-spoofing technologies (e.g., DKIM, DMARC, SPF), are not explicitly asserted as part of the proposal. Without enabling these technologies, .us emails may be subject to potential impersonation, including serving as a new mechanism for phishing consumers and businesses.

- **Email can be intercepted.**

  Mail system operators have full access to the contents of unencrypted mail messages. The operator's staff could read and use the contents of WHOIS mail, unknown to either the sender or recipient.

Requiring emails as the only mechanism to deliver the WHOIS data ignores other methods or protocols for delivering the data that exist today or that may exist in the future, and represents a step backward in providing internet services. In the gTLD space, the RDAP protocol is required for the delivery of WHOIS information in a machine-readable format. This allows for faster response to queries and enables higher volumes of legitimate queries to be processed. RDAP also allows for using web services, data encryption in transit, authentication, and access control methods that are widely incorporated into modern applications. Many ccTLDs have also adopted the RDAP standard.

(Element 4) Queries would be rejected only if the user did not provide a name and email address or failed to select (or provide) a legitimate purpose and accept the TOS.

As written, this means that a user could submit queries in unexpected formats or queries that are intentionally malformed. At the same time, we note that efforts to rate-limit or otherwise impose limits on volume (perhaps via tools like Captcha requirements) would impact on anti-abuse actors who often request relatively large amounts of data. It is not uncommon for malware networks to deploy thousands of domain names as part of the attack. If the agency proceeds with this proposal, we urge you to reconsider this blanket "query approval" standard.

(Element 5) The System would also permit users to identify a legitimate purpose outside of the pre-selected list. The Contractor using usTLD community developed and NTIA approved standards would manually review these requests and deliver, via email, unredacted data within two (2) business days for any non-abusive purpose unrelated to marketing.

We believe that a .us WHOIS policy with clear stipulations should cover all expected use cases and provide clear guidelines for approving uncommon requests. We appreciate that the proposal allows for flexibility and evolution. However, we would like to highlight some concerns:

1. It is unclear whether any newly approved purposes would be automatically added to the previously pre-populated list to ensure that others can avail themselves of "newly-deemed-appropriate purposes" on an even-handed basis. In our view, this should happen to achieve consistency.

2. It is unclear whether there will be any avenues for appeals of any denials. Usually, this should be possible and timely.
3. It is unclear whether marketing is the only forbidden purpose, and what the standards will be used for denying a stated purpose. This is why a clear and comprehensive policy is needed.
4. It is unclear whether there will be ample opportunity to provide additional information or attachments to justify the request. Some web forms adopted by registrars for WHOIS or domain name abuse requests impose unreasonable limits on the amount of explanatory text or content that can accompany the request.

However, we note that the administrative overhead and cost of managing an expanding list of legitimate purposes, as well as the cost overhead of falling on both the applicant and the Contractor, speaks to the value of approaching the issue from the other direction. In other words, all uses should be considered appropriate except a narrowly drawn list of inappropriate purposes.

(Element 6) The System would also provide a mechanism to expedite emergency requests.

In general, we support the concept of "exigent circumstances" mechanisms, but we do not understand the need for one, based on the proposal. While precise definitions of "exigent circumstances" may vary and would need to be settled upon by the Agency, we assume this means an emergency situation requiring swift action to prevent imminent danger to life or serious damage to property, or to forestall the imminent escape of a suspect, or the destruction of evidence.

However, it is currently unclear why this would be needed. As we understand the proposal, an emergency request would likely fall under the accepted purposes and should be answered in near real-time, either via email or other means (should they be established). Therefore, it is unclear why law enforcement or anti-abuse actors would have to file such requests at all.

(Element 7) Non-personal information relating to the domain name would remain available for retrieval via anonymous query. This information includes domain name and ID, registrar WHOIS server, registrar URL, updated date, creation date, registry expiry date, registrar, registrar IANA ID, and registrar abuse contact (email and phone number).

We prefer to see no change in policy to access all .us WHOIS information via classic port 43/TCP WHOIS, web WHOIS gateways, and RDAP, without redactions or other exclusions that are not required by applicable US law. Nevertheless, for information about real persons (rather than legal persons such as corporations), if withholding that data proves unavoidable, we recommend **hashing** the personal information rather than **redacting** it[9] as well as the creation of full data access schemes for private and government anti-abuse actors.

WHOIS information for corporations or other legal persons should be provided in the clear and without limits.

(Element 8) To address the unique needs of law enforcement and other similarly situated entities, the Contractor would establish a portal for authenticated law enforcement users, which would grant such users near real-time access to personal information. The Contractor would continue to work

[9] See https://www.icann.org/en/system/files/correspondence/jevans-to-marby-et-al-04jun18-en.pdf

with law enforcement authorities and others to ensure that investigatory confidentiality and unique other needs with respect to access and confidentiality are fully met.

Based on the currently available information, it is unclear why a special portal would be needed. The proposal states that legitimate requests would be answered in near real-time, making the creation of special access superfluous.

We also note that the proposed plan lacks specificity regarding what is meant by "similarly situated entities." For example, this category could include sworn American law enforcement officers with criminal power of arrest, as well as federal or state investigators and tribal investigators. This could also include members of the domestic or international intelligence community, which could raise unique concerns, such as whether there should be FISA Court oversight**.** It also could include international police officers, including officers from countries hostile to American interests, or officers from countries with a history of human rights abuse or corruption.

M[3]AAWG encourages the Agency to enable government and private cybersecurity professionals to have access to the portal, should one be established. Today, the overwhelming majority of the mitigation activities for phishing, malware, and other types of DNS abuse are performed by cybersecurity professionals in private organizations rather than by law enforcement. As a result, the proposal should be expanded to allow "trusted notifiers" to use the portal rather than the email system for access and disclosure of WHOIS information.

(Element 9) The Contractor would maintain auditable records of its receipt of and response to WHOIS access requests for personal data, including the number of access requests received, and the declared legitimate purposes. The Contractor would also maintain records to audit complaints of technical abuse or TOS violations. These audit records would be made publicly available in fully de-identified and aggregated form for analysis, enabling additional data-driven policy development by NTIA and the usTLD community.

We have doubts about the effectiveness of the attempts at de-identification and aggregation for anonymization. While that feature may be undertaken with both care and the best of intentions, it can be surprisingly easy for it to go wrong.[10] Instead, we suggest the production of an annual summary report modeled on the United States Court Wiretap report.[11]

We note that the accountability sought by the Agency focuses exclusively on the requester of the data and does not address the accuracy of data received from the registrant. M[3]AAWG suggests that the Agency consider verification rules from the data subject that submits WHOIS data to be registered in the .us registry.

[10] See, for example, "Your Data Were 'Anonymized'? These Scientists Can Still Identify You," https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html

[11] See, for example, https://www.uscourts.gov/statistics-reports/wiretap-report-2021

In conclusion, we appreciate the opportunity to submit these comments. We welcome the opportunity to engage 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
comments@m3aawg.org
P.O. Box 9125 Brea, CA 92822