Office of Inspector General
United States Department of State

ESP-20-05 | Office of Evaluations and Special Projects | September 2020

Management Assistance Report: U.S. Agency for Global Media Network Warning Banner

MANAGEMENT ASSISTANCE REPORT

Summary of Review

In connection with a recent criminal investigation and felony prosecution, the Office of Inspector General (OIG) reviewed the warning banners displayed by computers issued to employees of the U.S. Agency for Global Media (USAGM). This banner fails to meet applicable guidelines set forth by the Department of Justice's (DOJ) Computer Crimes and Intellectual Property Section (CCIPS) and by the National Institute of Standards and Technology (NIST). This deficiency creates the risk that law enforcement officers seeking to access information regarding use of USAGM computers and systems will be compelled to obtain a warrant to do so, thereby risking unnecessary delays and possible destruction or exclusion of evidence in criminal investigations. It may also limit USAGM's ability to administratively monitor the system usage of USAGM employees (or others on the USAGM network). OIG recommends that USAGM revise its banner in accordance with applicable CCIPS guidance and/or one of the models provided by CCIPS.

BACKGROUND

In 2019, OIG received allegations that a senior USAGM employee, Haroon Ullah, was engaging in abuse of official travel, including submitting false travel reimbursement requests that he created on his government computer. OIG opened an investigation into the allegations and sought access to Mr. Ullah's USAGM-issued computer, which OIG believed could contain evidence relevant to the allegations.

Employees of the federal government are routinely issued electronic devices (such as computers) and given access to government networks in order to carry out their job responsibilities. Although most federal employees use the electronic devices issued to them in accordance with these guidelines and with other relevant laws and policies, in rare instances, individuals such as Mr. Ullah use these devices to engage in conduct that violates agency policies or even criminal statutes. Accordingly, it is important for agency or OIG officials to be able to monitor and document misuse of government-owned electronic devices and networks quickly and efficiently, particularly because delays risk the potential destruction of evidence or the prolonging of potential abuses. In the case of potential criminal violations, agency or OIG officials are able to monitor and document misuse because courts have generally held that law enforcement officers need not engage in the often lengthy process of obtaining a warrant to retrieve the information stored on a government-owned electronic device or network.

However, courts have held that even when seeking access to government electronic devices or networks being used by government employees, law enforcement officers may only conduct a warrantless search and seizure when the user of the device or network could not have had a

"reasonable expectation of privacy" in the device or the information stored on it.[1] Whether the user could have had this reasonable expectation of privacy often turns on the warning or banner that is displayed when a user logs on to a device.[2]

CCIPS, which is responsible for implementing strategies to combat computer and intellectual property crimes, provides relevant guidance and case law summaries to federal prosecutors for making a determination regarding whether to seek a warrant in its manual, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (CCIPS Manual).[3] Further guidance is provided by NIST in its guidance *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST Guidance).[4] Because the USAGM banners were not phrased in a way that clearly conformed with this guidance, OIG sought a warrant to search Mr. Ullah's government computer. Under the circumstances, these steps unnecessarily prolonged the investigation of this matter.

FINDINGS

The current USAGM banner is pictured below.

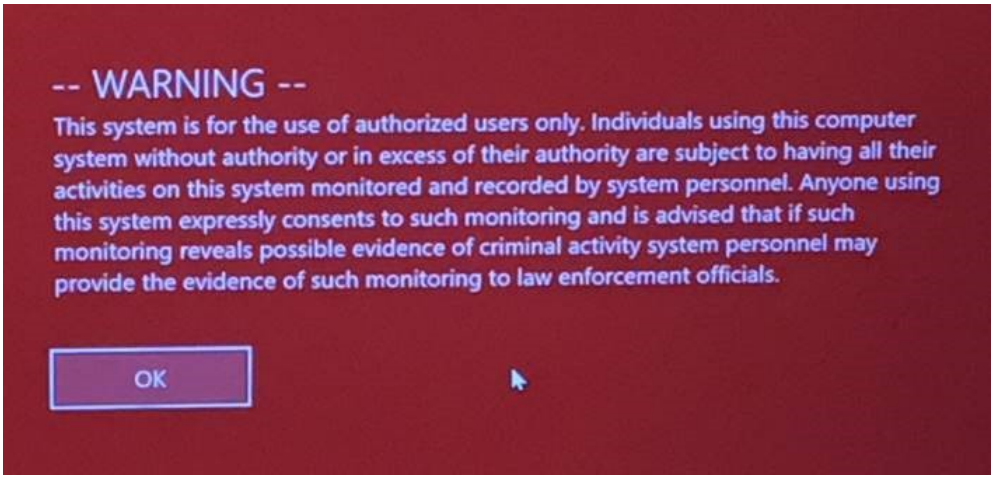


Figure 1: USAGM computer banner

[1] *United States v. Simons*, 206 F.3d 392, 395-98 (4th Cir. 2000) (holding that agency employee did not have reasonable expectation of privacy in his agency computer in light of displayed warning banners); *Biby v. Board of Regents*, 419 F.3d 845, 850-51 (8th Cir. 2005) (concluding that computer user had no reasonable expectation of privacy where policy stated records may be searched in response to discovery requests).

[2] CCIPS Manual at 49-50 (listing cases).

[3] Available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

[4] NIST Special Publication 800-53, Revision 4, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. This guidance is consistent with OMB Circular No. A-130, which, among other things, establishes the general policy for the governance and management of Federal information technology resources. OMB Circular A-130, "Managing Federal Information as a Strategic Resource," https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf (July 28, 2016).

After reading the warning set forth in Figure 1, users must click "OK" before proceeding to use the electronic device.

This banner is inconsistent with the NIST Guidance and CCIPS Manual in several material respects. First, the current USAGM banner does not specifically state that users of the system have no reasonable expectation of privacy in the system. A user who lacks a reasonable expectation of privacy in a network will probably not be able to succeed on a claim that any search of the network violates his or her Fourth Amendment rights.[5] The Fourth Amendment protects people from warrantless searches of their persons, houses, papers, and effects, provided they have a reasonable expectation of privacy in the area or item searched.

Similarly, the current USAGM banner fails to explicitly advise users that they are accessing a U.S. government system and that any of their activities may be monitored and recorded for any reason. The CCIPS Manual states that such an advisement is critical to ensure that users cannot claim they had a reasonable expectation of privacy in the device or system.[6] Although the USAGM banner does state that users are "subject to having all their activities on this system monitored and recorded by system personnel," it limits the scope of this advisement to users who use or access the system "without authority or in excess of their authority."[7] Under some interpretations of this language, users could argue that they would not be subject to monitoring even if they were using their systems to commit fraud or other crimes, provided that they did so using applications and data to which they had authorized access.[8]

For similar reasons, the limitations in the current USAGM banner also fail to adequately address the topic of consent to monitoring, because the notice is constructed in such a way that suggests that only individuals accessing the system "without…or in excess of their authority" have consented to this monitoring. Both the NIST Guidance and CCIPS Manual state that

[5] *See e.g., Rakas v. Illinois*, 439 U.S. 128, 143 (1978) (stating that an individual who lacks reasonable expectation of privacy has no colorable Fourth Amendment claim).

[6] CCIPS Manual at 48-49 (citing *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000)).

[7] Notably, these are terms of art under the Computer Fraud and Abuse Act and relevant CCIPS guidance, which state that committing fraud on a government computer system to which an individual otherwise has authorized access might not necessarily fall within the definition of "without authority or in excess of their authority." The term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

[8] This issue is further compounded by the absence of any statement in the current USAGM banner regarding potential unscheduled system audits; including such a notification could further undermine any claim by a defendant of reasonable expectation of privacy. As noted elsewhere in this report, a defendant who lacks a reasonable expectation of privacy is unlikely to prevail on a claim that his or her Fourth Amendment rights were violated by warrantless search.

warning banners should explicitly include a statement that use of the system is equivalent to consent to monitoring. This provides not only direct consent but also supports a conclusion that users of government networks and electronic devices could not have had a reasonable expectation of privacy in their use of the system. The CCIPS Manual specifically highlights this issue and notes that such language helps establish the user's consent to real-time interception under the Electronic Communications Privacy Act, which allows for monitoring by law enforcement with consent.[9] As noted above, while the current USAGM banner does address the topic of consent, by suggesting that only individuals using the system "without…or in excess of their authority" consent to such monitoring, it arguably excludes individuals who access the system for authorized purposes but use it to carry out illegal activities (e.g., falsification of otherwise legitimate travel reports or time card fraud).

Finally, the current USAGM banner fails to advise the user that unauthorized use is prohibited and subject to criminal and civil penalties. Both the NIST Guidance and CCIPS Manual state that this information should be included.[10] Such a notice can help to establish knowledge of unauthorized use and thereby aid prosecution under the Computer Fraud and Abuse Act.[11]

USAGM can efficiently address these deficiencies by using one of the model banners that CCIPS includes in the CCIPS Manual.[12] These banners are used by other government agencies, including the Department of State, to ensure federal employees understand that their use of agency computers is subject to monitoring.[13]

---

[9] CCIPS Manual at 170-71. The relevant provision reads, "It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(c).

[10] In addition, the current USAGM banner states that, to the extent evidence of criminal activity is detected, system personnel "may" provide that evidence to law enforcement officials. Thus, if the monitor finds evidence of a crime, he or she may (or may not) choose to provide that to law enforcement. This language conflicts with the requirement in the Foreign Affairs Manual requiring all USAGM employees to report "known or suspected waste, fraud, abuse, false certifications, and corruption on a timely basis" to OIG, which is a law enforcement entity. 1 FAM 053.2-5 (Sept. 10, 2018).

[11] 18 U.S.C. § 1030.

[12] These model banners are in Appendix A of the CCIPS Manual.

[13] For example, the Department of State uses a banner that states: "You are about to enter a Department of State computer system or network. Use by unauthorized persons, or for unauthorized personal business, is prohibited and may constitute a violation of 18 U.S.C. 1030 and other Federal law, as well as applicable Department policies and procedures. You have NO REASONABLE EXPECTATION OF PRIVACY while using this computer system or network. All data contained and/or activities performed herein may be monitored, intercepted, recorded, read, copied, or captured in any manner by authorized personnel. System management personnel or supervisors may give law enforcement officials or appropriate Department managers any potential evidence of crime, fraud, or employee misconduct found on this computer system or network, and employees may be subject to discipline for misuse. Furthermore, law enforcement officials may be authorized to access and collect evidence from this

For example, the CCIPS Manual suggests the following language:

> You are accessing a U.S. Government information system, which includes this computer, this computer network, all computers connected to this network, and all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you understand and consent to the following: you have no reasonable expectation of privacy regarding communications or data transiting or stored on this information system; at any time, and for any lawful government purpose, the Government may monitor, intercept, search, and seize any communication or data transiting or stored on this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.[14]

Use of one of CCIPS's banners would give USAGM a powerful tool to ensure that misuse of its technology is promptly identified and addressed and would help to facilitate any future investigations of misuse of USAGM technology resources.

RECOMMENDATION

OIG makes one recommendation to USAGM. Its complete response can be found in the appendix.

Recommendation: The U.S. Agency for Global Media should adopt a network warning banner consistent with the guidance issued by the Department of Justice's Computer Crime and Intellectual Property Section.

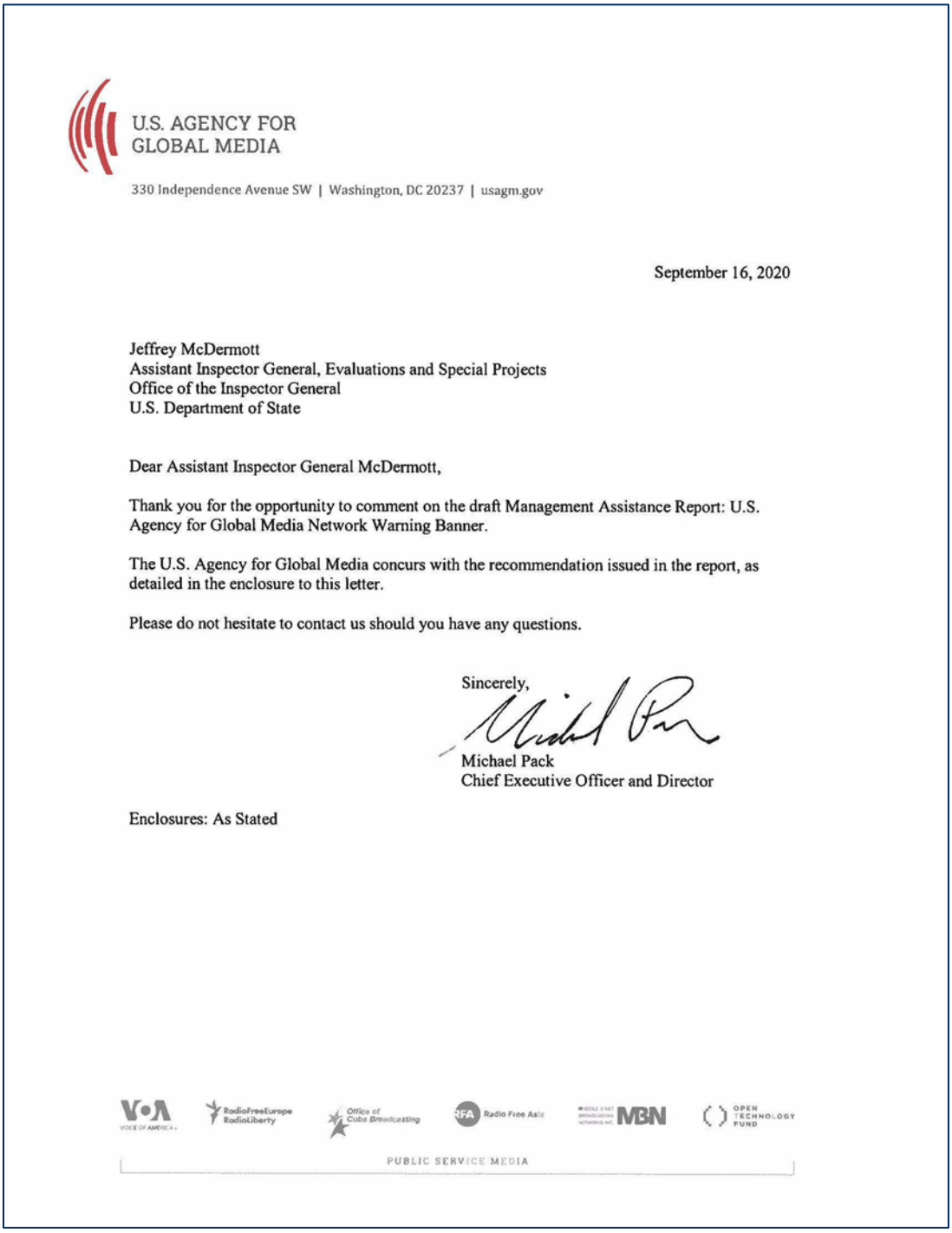
Management Response: In its September 16, 2020, response, the U.S. Agency for Global Media concurred with this recommendation.

OIG Reply: This recommendation can be closed when OIG receives documentation that the U.S. Agency for Global Media has updated its banner.

computer system or network, or from any portable devices that have been connected to this computer system or network. Therefore: USE OF THIS COMPUTER SYSTEM OR NETWORK BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES EXPRESS CONSENT TO THIS MONITORING. IF YOU DO NOT CONSENT TO THIS MONITORING, OR IF YOU ARE NOT AN AUTHORIZED USER, PRESS CTRL/ALT/DELETE SIMULTANEOUSLY AND EXIT THIS SYSTEM. IF YOU ARE AN AUTHORIZED USER AND CONSENT, PRESS OK (or RETURN, or ENTER) TO INDICATE YOU AGREE TO ALL THE CONDITIONS STATED HEREIN." 12 FAM 642.4-3 (July 16, 2008).

[14] CCIPS Manual at Appendix A.

APPENDIX: USAGM RESPONSE



U.S. AGENCY FOR GLOBAL MEDIA

330 Independence Avenue SW | Washington, DC 20237 | usagm.gov

September 16, 2020

Jeffrey McDermott
Assistant Inspector General, Evaluations and Special Projects
Office of the Inspector General
U.S. Department of State

Dear Assistant Inspector General McDermott,

Thank you for the opportunity to comment on the draft Management Assistance Report: U.S. Agency for Global Media Network Warning Banner.

The U.S. Agency for Global Media concurs with the recommendation issued in the report, as detailed in the enclosure to this letter.

Please do not hesitate to contact us should you have any questions.

Sincerely,

Michael Pack
Chief Executive Officer and Director

Enclosures: As Stated

VOA · RadioFreeEurope RadioLiberty · Office of Cuba Broadcasting · Radio Free Asia · MBN · Open Technology Fund

PUBLIC SERVICE MEDIA

Management Assistance Report: U.S. Agency for Global Media Network Warning Banner (ESP-20-XX)
September 3, 2020

Recommendation: The U.S. Agency for Global Media should adopt a network warning banner consistent with the guidance issued by the Department of Justice's Computer Crime and Intellectual Property Section.

Management Response: USAGM concurs with the recommendation to adopt a network warning banner consistent with guidance issued by the Department of Justice's Computer Crime and Intellectual Property Section.

HELP FIGHT

FRAUD, WASTE, AND ABUSE

1-800-409-9926
Stateoig.gov/HOTLINE

If you fear reprisal, contact the
OIG Whistleblower Coordinator to learn more about your rights.
WPEAOmbuds@stateoig.gov