Office of Inspector General
United States Department of State

ESP-20-03 Office of Evaluations and Special Projects March 2020

Management Assistance Report: Foreign Service Institute Wireless User Access Controls

SUMMARY OF REVIEW

The Foreign Service Institute (FSI) lacks modernized user access controls for its dedicated wireless network. The Office of Inspector General (OIG) recently became aware of this vulnerability during the course of a criminal investigation. OIG examined FSI's wireless user access controls and found that they do not comply with the wireless security standards of the Department of State (Department). In addition, OIG found that FSI could improve detection of unusual wireless network activities by implementing the Department's wireless access control protocols.

BACKGROUND

FSI is charged with the professional development and training of Department employees and the entire U.S. government foreign affairs community. FSI's main campus is located in Arlington, Virginia and offers nearly 600 on-campus courses. In this academic setting, the make-up of FSI employees, students, and guests routinely changes.

FSI information technology (IT) officials noted that, in approximately 2014, they decided that an "open" connection to its guest wireless network on the main campus was the most appropriate user access policy based on convenience for users. Therefore, FSI's access protocols are structured to allow any person within the campus boundaries to connect a mobile device directly to this network. These 5-year old protocols remain in effect today.

During a recent investigation, OIG became aware that a former FSI employee inappropriately used the FSI guest wireless network and relied upon its open connection to the internet to engage in criminal activity, and in at least some instances, he used his Department-issued mobile phone to do so.

FINDINGS

Department's Wi-Fi Access Standards

The Department's wireless standards are set by the Wi-Fi Governance Board (WFGB), co-chaired by the Bureau of Information Resource Management (IRM) and Bureau of Diplomatic Security (DS). The WFGB was established to provide oversight and approval over the implementation of wi-fi networks in the Department, both domestic and overseas. In 2013, the WFGB published *Wireless Local Area Network (WLAN) Security Standard for Dedicated Internet Networks (DIN)*, which sets conditions for wi-fi networks that must be met before activation, as well as maintained throughout their lifecycle.[1] These standards, which were updated in 2017, were designed to prevent risks associated with wireless networks. These risks can include

[1] Department of State, Bureau of Diplomatic Security, Office of Cybersecurity, *Wireless Local Area Network (WLAN) Security Standard for Dedicated Internet Networks (DIN)* (version 2.0, May 2017).

compromised confidentiality, integrity, and availability of Department information and systems; decreased productivity; and damaged Department information assets.

According to these standards, a wireless network must include an appropriate user registration mechanism that electronically captures the user's properly formatted email address and explicitly requires the user to agree to the outlined legal disclosures and disclaimers.[2]

These standards also require that wireless networks be segmented by connection type. To illustrate, a Department wireless network must have two segments – one segment that only permits connection of registered Government-owned mobile devices and a separate segment for the connection of personally-owned devices. Network segmentation improves cyber security by decreasing the possibility of unauthorized access to Department information.

FSI's Wireless Network

As part of its open connection approach, FSI grants wireless internet access to any on-campus user who clicks on the Terms and Use Agreement acceptance box found on its opening login page. However, the FSI guest network does not comply with the WFGB requirement that the system capture a user's properly formatted email address.[3] Therefore, FSI cannot determine who made any particular connection because its access controls do not require users to take steps to identify themselves prior to the start of a wireless session. The failure to capture such information makes it more difficult to identify individuals, such as the FSI employee in question, who misuse the wireless network. OIG notes that compliance with the WFGB requirement would not preclude FSI's "open connection" approach, as FSI could still grant access to anyone so long as he or she entered a valid email address.

Similarly, the FSI wireless network simultaneously handles internet connections from both Department-owned mobile devices and personally owned mobile devices without the network segmentation required by the WFGB standards. As noted previously, failure to segment networks used by Department-owned and personal devices increases risks to Department information. In addition, segmentation is beneficial because it helps to identify and monitor users who connect to the network using a Department-issued device. If FSI's wireless network had been segmented, FSI may have been able to identify when the FSI employee in question connected to it using his Department-issued mobile phone. Moreover, his activities on that device would have been more visible and more easily monitored, because his phone would have been programmed to connect specifically to the Department-owned device access point, and the connection of his device would have been immediately logged.

[2] According to IRM officials, they are in the process of updating the standards to require two-factor authentication for users to access a wireless network, an approach that will further protect wireless networks.

[3] During this review, OIG became aware that other Department wireless networks, such as the one in the Department's main cafeteria, are also not in compliance with this standard. In its response, FSI stated that it understands that IRM plans to update its access controls in the cafeteria.

RECOMMENDATION

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

Recommendation 1: The Foreign Service Institute should ensure that its guest wireless network complies with the Department's wireless security standards.

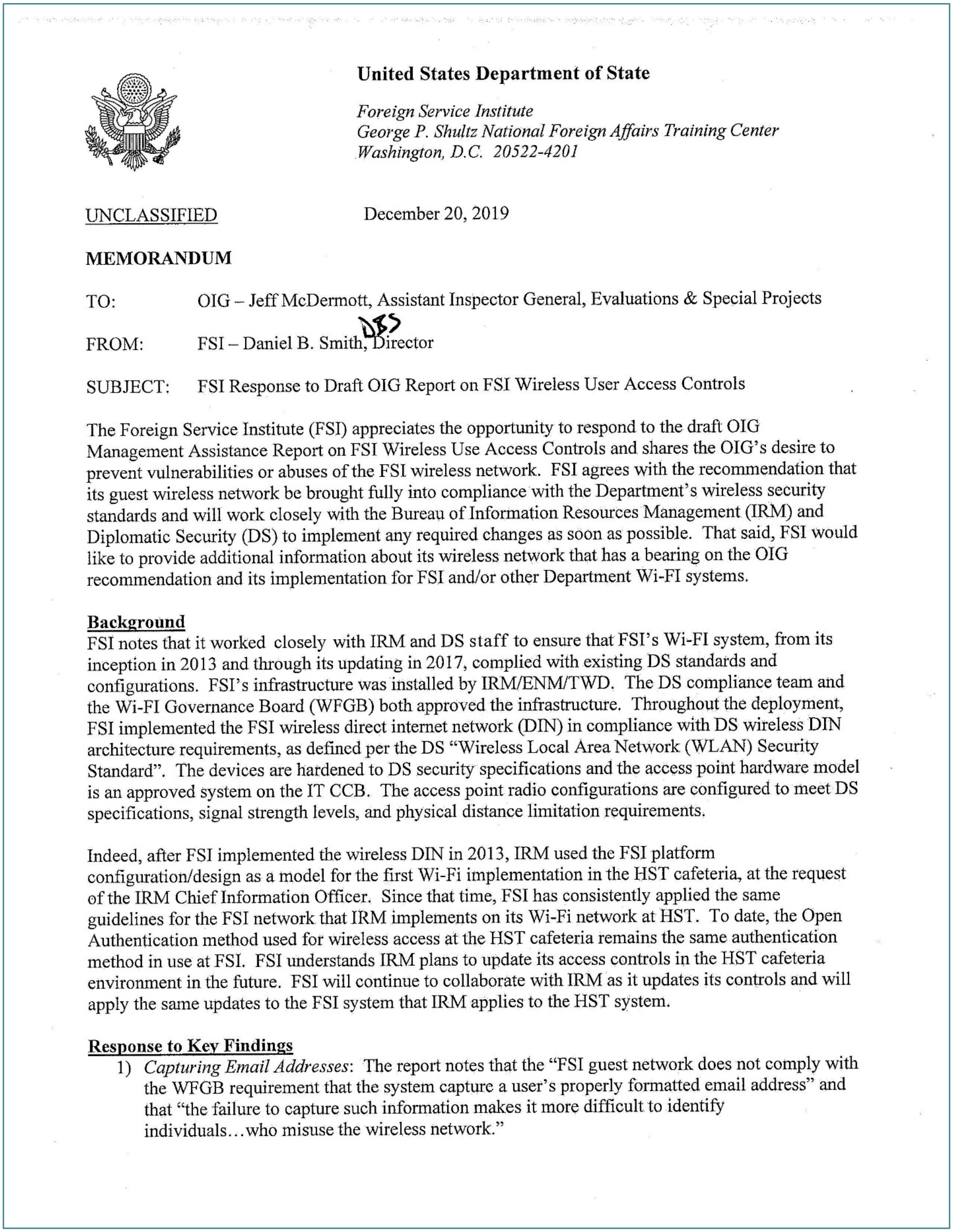
Management Response: In its December 20, 2019, response, the Foreign Service Institute concurred with this recommendation and stated that it will work with the Bureaus of Information Resource Management and Diplomatic Security to ensure that its wireless network complies with Department standards.

Notwithstanding its concurrence, FSI asserted that the collection of email addresses without taking additional steps would not allow it to identify users who misuse the wireless network. It stated that it does not have the resources to take these additional steps.

FSI also asserted in its response that its wireless network is in compliance with the WFGB standards on segmentation because the standards only require network segmentation when a wireless network is integrated with an existing network infrastructure that provides distinctly independent services (e.g., access to other Department web servers or Department email), or when the wireless infrastructure provides access to both Department-owned and public networks. According to FSI, its wireless network is completely separate from all other Department resources.

OIG Reply: This recommendation can be closed when OIG receives documentation that the Foreign Service Institute guest wireless network complies with the Department's wireless security standards. Regarding FSI's assertion that it does not have the capacity to take the additional steps that would allow it to identify users who misuse the wireless network, the requirement to enter an email address would nonetheless likely have some deterrent effect in discouraging misuse of the network, and as noted, is required by the WFGB standards. OIG disagrees with FSI's assertion that its wireless network is properly segmented. The WFGB standards state that wireless infrastructure that provides access to both Department-owned devices and public networks must, at minimum, logically maintain complete separation of the independent traffic streams. FSI uses Department-owned devices on its wireless network and offers Internet access to personal devices, yet it does not maintain separation of these traffic streams.

APPENDIX: FSI RESPONSE



United States Department of State

Foreign Service Institute
George P. Shultz National Foreign Affairs Training Center
Washington, D.C. 20522-4201

UNCLASSIFIED December 20, 2019

MEMORANDUM

TO: OIG – Jeff McDermott, Assistant Inspector General, Evaluations & Special Projects

FROM: FSI – Daniel B. Smith, Director DBS

SUBJECT: FSI Response to Draft OIG Report on FSI Wireless User Access Controls

The Foreign Service Institute (FSI) appreciates the opportunity to respond to the draft OIG Management Assistance Report on FSI Wireless Use Access Controls and shares the OIG's desire to prevent vulnerabilities or abuses of the FSI wireless network. FSI agrees with the recommendation that its guest wireless network be brought fully into compliance with the Department's wireless security standards and will work closely with the Bureau of Information Resources Management (IRM) and Diplomatic Security (DS) to implement any required changes as soon as possible. That said, FSI would like to provide additional information about its wireless network that has a bearing on the OIG recommendation and its implementation for FSI and/or other Department Wi-FI systems.

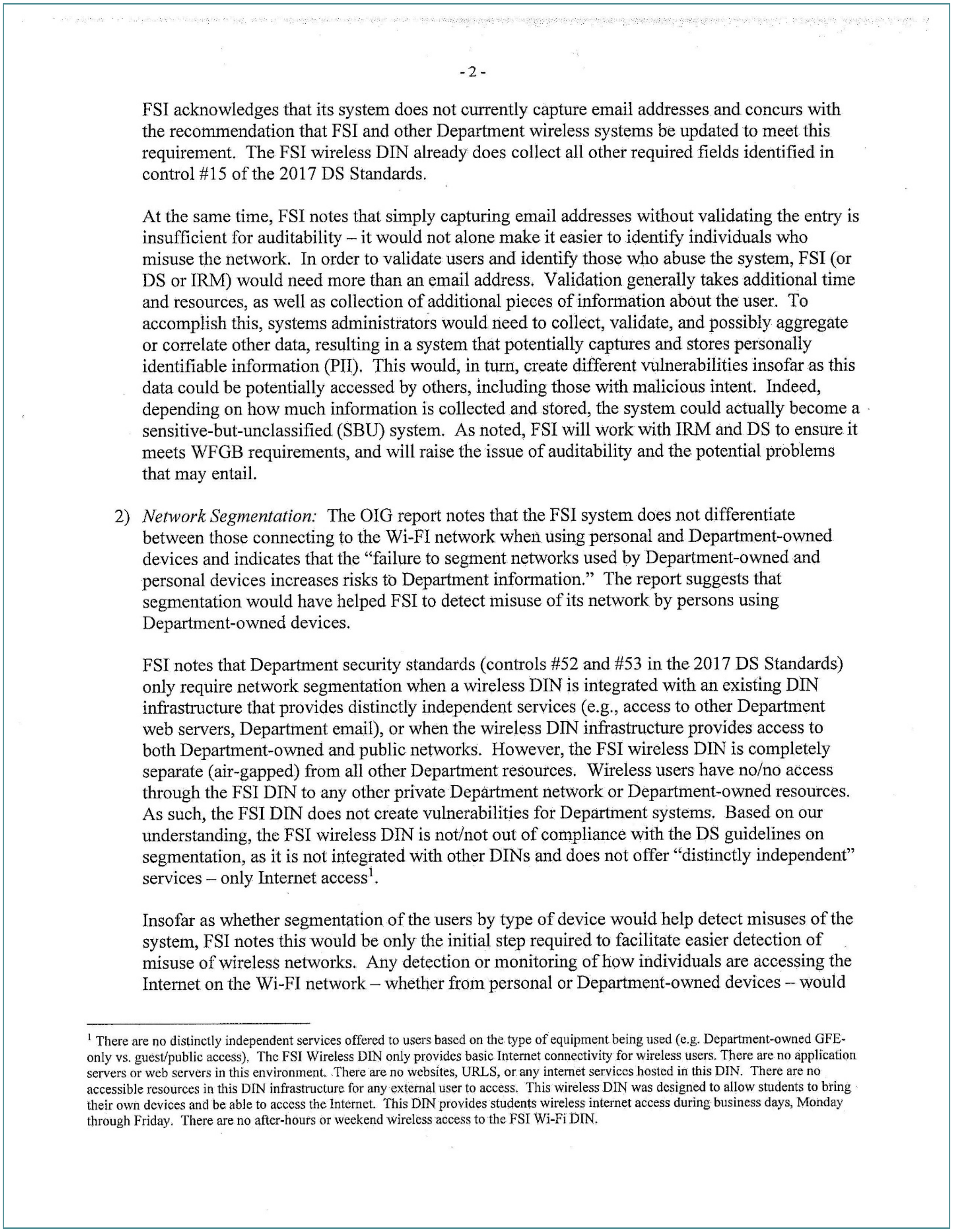
Background

FSI notes that it worked closely with IRM and DS staff to ensure that FSI's Wi-FI system, from its inception in 2013 and through its updating in 2017, complied with existing DS standards and configurations. FSI's infrastructure was installed by IRM/ENM/TWD. The DS compliance team and the Wi-FI Governance Board (WFGB) both approved the infrastructure. Throughout the deployment, FSI implemented the FSI wireless direct internet network (DIN) in compliance with DS wireless DIN architecture requirements, as defined per the DS "Wireless Local Area Network (WLAN) Security Standard". The devices are hardened to DS security specifications and the access point hardware model is an approved system on the IT CCB. The access point radio configurations are configured to meet DS specifications, signal strength levels, and physical distance limitation requirements.

Indeed, after FSI implemented the wireless DIN in 2013, IRM used the FSI platform configuration/design as a model for the first Wi-Fi implementation in the HST cafeteria, at the request of the IRM Chief Information Officer. Since that time, FSI has consistently applied the same guidelines for the FSI network that IRM implements on its Wi-Fi network at HST. To date, the Open Authentication method used for wireless access at the HST cafeteria remains the same authentication method in use at FSI. FSI understands IRM plans to update its access controls in the HST cafeteria environment in the future. FSI will continue to collaborate with IRM as it updates its controls and will apply the same updates to the FSI system that IRM applies to the HST system.

Response to Key Findings

1) *Capturing Email Addresses*: The report notes that the "FSI guest network does not comply with the WFGB requirement that the system capture a user's properly formatted email address" and that "the failure to capture such information makes it more difficult to identify individuals…who misuse the wireless network."



FSI acknowledges that its system does not currently capture email addresses and concurs with the recommendation that FSI and other Department wireless systems be updated to meet this requirement. The FSI wireless DIN already does collect all other required fields identified in control #15 of the 2017 DS Standards.

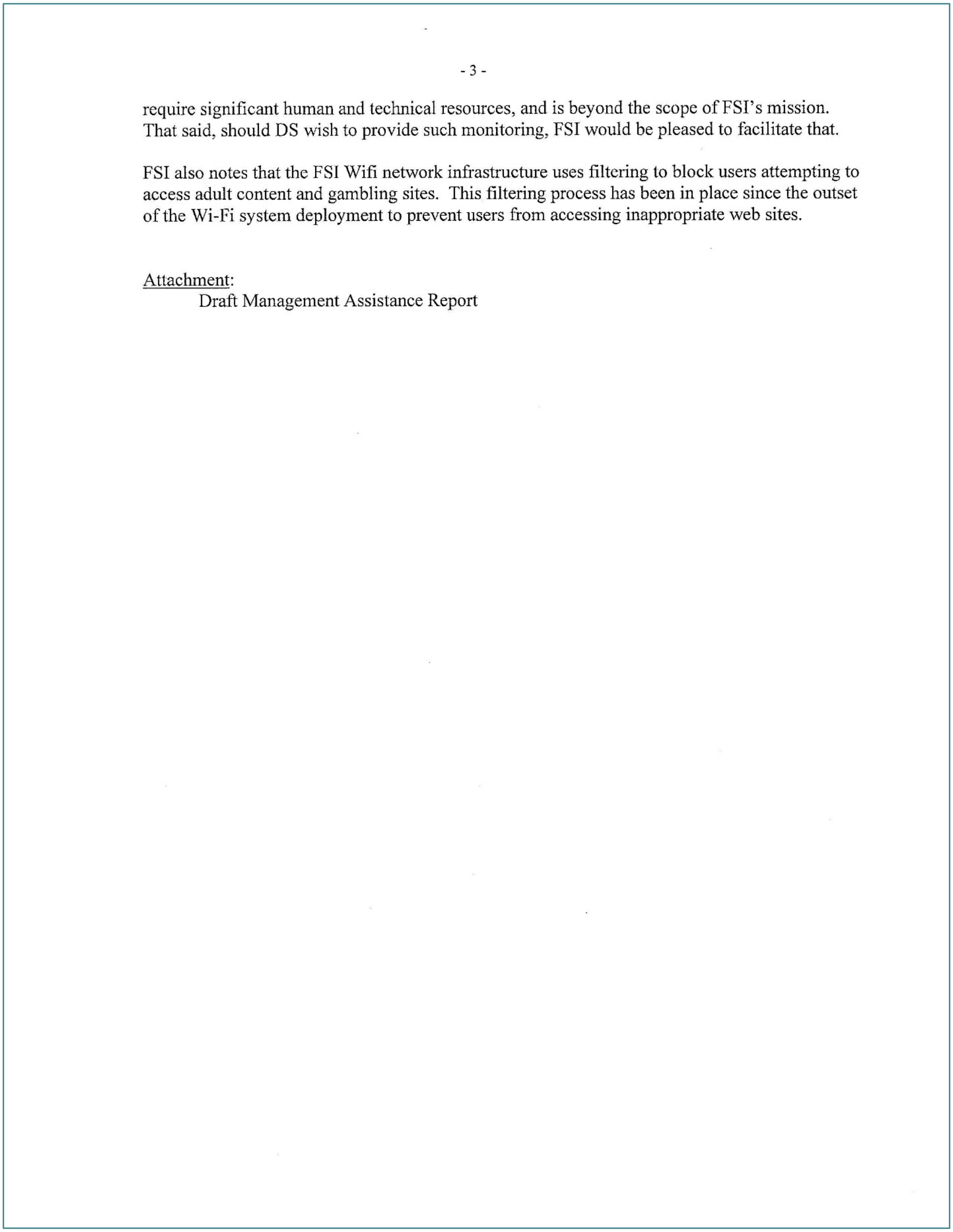
At the same time, FSI notes that simply capturing email addresses without validating the entry is insufficient for auditability – it would not alone make it easier to identify individuals who misuse the network. In order to validate users and identify those who abuse the system, FSI (or DS or IRM) would need more than an email address. Validation generally takes additional time and resources, as well as collection of additional pieces of information about the user. To accomplish this, systems administrators would need to collect, validate, and possibly aggregate or correlate other data, resulting in a system that potentially captures and stores personally identifiable information (PII). This would, in turn, create different vulnerabilities insofar as this data could be potentially accessed by others, including those with malicious intent. Indeed, depending on how much information is collected and stored, the system could actually become a sensitive-but-unclassified (SBU) system. As noted, FSI will work with IRM and DS to ensure it meets WFGB requirements, and will raise the issue of auditability and the potential problems that may entail.

2) *Network Segmentation:* The OIG report notes that the FSI system does not differentiate between those connecting to the Wi-FI network when using personal and Department-owned devices and indicates that the "failure to segment networks used by Department-owned and personal devices increases risks to Department information." The report suggests that segmentation would have helped FSI to detect misuse of its network by persons using Department-owned devices.

FSI notes that Department security standards (controls #52 and #53 in the 2017 DS Standards) only require network segmentation when a wireless DIN is integrated with an existing DIN infrastructure that provides distinctly independent services (e.g., access to other Department web servers, Department email), or when the wireless DIN infrastructure provides access to both Department-owned and public networks. However, the FSI wireless DIN is completely separate (air-gapped) from all other Department resources. Wireless users have no/no access through the FSI DIN to any other private Department network or Department-owned resources. As such, the FSI DIN does not create vulnerabilities for Department systems. Based on our understanding, the FSI wireless DIN is not/not out of compliance with the DS guidelines on segmentation, as it is not integrated with other DINs and does not offer "distinctly independent" services – only Internet access[1].

Insofar as whether segmentation of the users by type of device would help detect misuses of the system, FSI notes this would be only the initial step required to facilitate easier detection of misuse of wireless networks. Any detection or monitoring of how individuals are accessing the Internet on the Wi-FI network – whether from personal or Department-owned devices – would

[1] There are no distinctly independent services offered to users based on the type of equipment being used (e.g. Department-owned GFE-only vs. guest/public access). The FSI Wireless DIN only provides basic Internet connectivity for wireless users. There are no application servers or web servers in this environment. There are no websites, URLS, or any internet services hosted in this DIN. There are no accessible resources in this DIN infrastructure for any external user to access. This wireless DIN was designed to allow students to bring their own devices and be able to access the Internet. This DIN provides students wireless internet access during business days, Monday through Friday. There are no after-hours or weekend wireless access to the FSI Wi-Fi DIN.



require significant human and technical resources, and is beyond the scope of FSI's mission. That said, should DS wish to provide such monitoring, FSI would be pleased to facilitate that.

FSI also notes that the FSI Wifi network infrastructure uses filtering to block users attempting to access adult content and gambling sites. This filtering process has been in place since the outset of the Wi-Fi system deployment to prevent users from accessing inappropriate web sites.

Attachment:
Draft Management Assistance Report

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