THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON

September 5, 2025

The Honorable Jamieson Greer
Acting Special Counsel
U.S. Office of Special Counsel
1730 M Street, NW, Suite 300
Washington, DC 20036

Dear Ambassador Greer:

I am responding to your April 1, 2025, request for a supplemental report to the Office of the Inspector General's (OIG) investigation regarding whistleblower disclosure of a violation of law, rule, or regulation, gross mismanagement, and a substantial and specific danger to public health at the Lieutenant Colonel Charles Kettles VA Medical Center in Ann Arbor, Michigan.

The Veterans Health Administration and OIG addressed the questions as posed in your office's request. The completed supplemental report is enclosed.

Thank you for the opportunity to respond.

Sincerely,

Douglas A. Collins

Enclosure

Department of Veterans Affairs (VA)
White Paper for the Office of Special Counsel (OSC)
File No. 24-000312, Ann Arbor

The Office of the Secretary of the Department of Veterans Affairs (VA) received an email from OSC on April 1, 2025, requesting a supplemental report addressing questions about the VA's Office of the Inspector General (OIG) Report of Investigation re OSC Referral DI-24-000312. The Veterans Health Administration (VHA), along with the OIG, provides the responses below to OSC's questions.

Question 1: How is the call schedule documenting which attending surgeon(s) are on call each day disseminated and/or posted for employees who may need to use it?

VA Response: The administrative staff in the Surgery Service updates the monthly surgical faculty/resident team information and posts the VA Ann Arbor Call Schedules on the facility SharePoint website for staff to access. Surgery paging and the on-call contacts are also accessible from the affiliate paging website (University of Michigan) that is accessible through the VA Ann Arbor network.

Question 2: The investigation found that there is no documented, formal policy outlining the communication escalation procedure for on call providers – has a formal policy since been created?

1. **If so, please provide it.**
2. **If not, please explain why.**

VA Response: No, a formal policy outlining the communication escalation procedure for on-call providers was not created. VA Ann Arbor follows the on-call guidelines set forth in VHA Directive 1220(1) and ensures on-call schedules are available to staff as described in the response to question 1. To supplement these resources, the attached "Surgical Services Escalation Pathway" tool was developed in April 2023. This resource was available at the time of OIG's investigation but has since been reviewed with staff and is now posted with the VA Ann Arbor call schedules on the facility SharePoint.

Question 3: The investigation found that because the facility is continuously staffed by hospitalists, then the facility consistently has "qualified inpatient coverage in house for all patients" because hospitalists meet the requirement for in-house coverage under VHA Directive 1220(1). Per VHA Directive 1400.01 (Section 8(b)(1)(a-d)), if a hospitalist is acting as the supervising practitioner, then they are required to document their involvement in care through one of four options provided in the Directive. The options include:

(i) entry into the health record by the supervising practitioner;
(ii) addendum to the health record entry by the supervising practitioner;
(iii) co-signature of the health record entry by the supervising practitioner; or
(iv) reference to the supervising practitioner within the health record entry.

Of the daily surgical health record entries for the cases investigators reviewed, how many satisfied one of the four requirements?

VA Response (provided by OIG): None of the seven patient records reviewed met any of the four requirements. The limited review of four patient records did not satisfy any of the requirements for documentation by an in-house supervising practitioner during off-tour hours. The other three patient records reviewed were not applicable.

Question 4: In its report, the OIG noted that the way in which the facility is currently monitoring the documentation of complex and high-risk surgical procedures may result in inaccurate compliance data – could you please provide more information about the agency's plan to ensure surgical procedures are being properly documented and the resulting compliance data is accurate?

VA Response: VA Ann Arbor leadership reviewed and updated the process for monitoring documentation of complex and high-risk surgical procedures. Effective October 2024, the Associate Chief Nurse, Surgery and Perioperative Service now completes a retrospective review of 100% of surgical cases to assess compliance with post-operative documentation. Audit results are reviewed and discussed monthly at the facility Surgical Work Action Group and Surgical Section Chief meetings.

Question 5: The report substantiated the whistleblower's allegation that physician residents without approved credentials accessed the VA computer system – did the investigators identify any corresponding violation of federal law?

a. **Namely, please indicate whether investigators identified a violation of 18 U.S.C. § 1030, the Computer Fraud and Abuse Act.**
    i. **If not, why?**
    ii. **If so, please indicate what responsive actions are being taken.**

VA Response (provided by OIG): No, the health care inspection team did not consider any violation of Federal law, namely, 18 U.S.C. § 1030,[1] fraud, and related activity in connection with computers (also known as the Computer Fraud and Abuse Act of 1986 (CFAA)), given the circumstances in this matter. Although OIG substantiated the unauthorized use of the VA computer system by physician resident trainees (trainees), access was provided to the trainees to allow a timely start of their clinical rotation at the facility and facilitate the provision of care and treatment to patients without delay, even though the vetting of the trainees' credentials had not yet been completed by the

[1] Pursuant to 18 U.S.C. § 1030(a)(1) a violation of the law occurs when a person(s) "having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the Unitedhttps://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=18-USC-80204913-692694673&term_occur=999&term_src= States Government to require protection against unauthorized disclosure … with reason to believe that such information so obtained could be used to the injury of the United States, willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to anyhttps://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=18-USC-991716523-1301629&term_occur=999&term_src= not entitled to receive it."

facility.[2] There was no evidence of any intent to defraud the United States through the computer access, and access was granted to the trainees by the responsible attending physicians. No evidence of criminality or improper intent as described in the CFAA (such as computer hacking, obtaining information for nefarious or fraudulent purposes) was identified.

While VHA requires that all facilities follow applicable administrative, technical, and physical safeguards to ensure the security and confidentiality of personally identifiable information and records, including in VA computer systems, there were facility process issues that prevented timely completion of the required vetting of trainee credentials before the start of their clinical rotations. To assist trainees who were commencing their rotation without authorized computer access, a work-around was implemented that involved an attending physician (supervising practitioner) logging onto the computer under their credentials and allowing the trainee to access the computer and related databases until the trainee obtained authorized access. This was reportedly done for purposes of facilitating a trainee's clinical rotation with review of patient records and to document the care provided. This unauthorized practice was limited to anesthesia attending physicians in the operating room; other departments the inspection team queried were not found to be implementing this practice.

OIG further learned that an anesthesia attending periodically left the operating room, thus leaving the trainee with unmonitored computer access. The trainee could potentially have exceeded their "authorized access"[3] by entering those areas in the computer not otherwise authorized and obtaining information. However, the inspection team was not informed of any such occurrences. Additionally, there is concern that any incorrect information documented by the trainee in a patient's medical records would be attributed to the anesthesia attending; this creates other legal and ethical concerns, especially as the attending did not author the note and the trainee's identity would not be recorded.

The anesthesia trainees' unauthorized access to VA computers violated VHA policy. Although these trainees "knowingly accessed a [VA] computer without the [required VHA] authorization,"[4] they were provided authorized access under the direction of the anesthesia attending despite not being properly vetted for gaining such access. The OIG inspectors deemed the unauthorized computer access by the anesthesia trainees a serious concern and breach of established protections and safeguards of

---

[2] Resolution times for obtaining authorized computer access varied.

[3] Van Buren v. United States, 593 U.S. 374, 141 S. Ct. 1648, 1652, 210 L. Ed. 2d 26 (2021) (holding that 18 U.S.C. § 1030 applies when a person accesses a computer with authorization but then obtains information located in particular areas of that computer—such as files, folders, or databases—to which their computer access did not extend; it does not cover those with improper motives for obtaining information that was otherwise available to them). In Van Buren, the Petitioner was a police officer who was authorized to use his computer to access and retrieve license-plate information but obtained information from the database for an improper use. The Court held that "since the parties agreed that a police officer was allowed to use the system to retrieve the information, he did not exceed authorized access to the database, as the Computer Fraud and Abuse Act of 1986 defined that phrase, even though he had obtained information for an improper use." Id. See also 18 U.S.C. § 1030(e)(6) (providing that '"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."

[4] 18 U.S.C. § 1030(a)(1).

sensitive information and the VA computer system. But due to the untimely completion for vetting trainees' credentials by the facility for trainees to gain authorized computer access for their rotation, interim computer access was provided to facilitate their training and delivery of patient care. The inspection team was not informed of any impaired integrity of data or harm to the computer system.

Upon learning of the unauthorized access of VA computers by trainees, OIG health care inspection team immediately informed the facility Chief of Staff of this finding as well as facility and Veterans Integrated Services Network leaders during the on-site inspection. The inspection team also spoke with Office of Academic Affiliations leaders who informed OIG that the concerns were relayed to VHA leaders. The difficulty with obtaining computer access for trainees across VA facilities remains an ongoing concern at both the VISN and national levels.

Department of Veterans Affairs
September 2025

SURGICAL SERVICE COMMUNICATION AND ESCALATION OF CONCERNS POLICY

PAGING IS ACCESSED FROM VA THROUGH UM PAGING FOR AFFILIATE ACESS:
https://uhmspaging.med.umich.edu/homePaging/PagingSend/search.aspx

RESIDENT ON CALL (UM PAGER # IN RED) → VA CHIEF RESIDENT ON CALL (WHEN DIFFERENT FROM RESIDENT ON CALL) → ATTENDING (SURGICAL ATTENDING OF RECORD) → SECTION CHIEF (ATTENDING PHYSICIAN) → CHIEF OF SURGERY → CHIEF OF STAFF

Expectation for timeliness:

1. **Emergent/ASAP - Immediately**
2. **Urgent – expected call back and response within 5min (same at each level) - (If escalating calls- please re-page the prior call as well as next step)**
3. **Routine (order clarification) – call back within 30 min (Re-page if no response within 30 min)**

Definition of emergent calls- Time sensitive patient care requiring intervention (Examples - hypotension, neuro status changes, bleeding)

Airway emergencies and Codes would still activate Code team
Rapid Response calls outside the ICU remain the same.

General Surgery and Vascular Surgery Pager: **33781**	**Urology Pager:** Inpatients on urology service: **39048** Consults-inpatients and ER: **39049**
ENT Head/Neck Pager: **35830**	**CT Surgery Pager:** **53963**
Neurosurgery Pager: **35354**	**Opthomology Pager:** **9342**
Plastic Surgery Pager: **34407**	**Surgical Intensivists Pager:** **39087**
Orthopedic Surgery Pager: **34503**	

- **When Escalating to section chief please inform the charge nurse. Phone numbers for Section Chiefs are listed in the ICU huddle sheet folder.**
- **When Escalating to Chief of Staff (COS) please call House Supervisors and go through AOD for COS number.**

MRR 4.11.23
AKB 4.19.23