ONE HUNDRED SIXTEENTH CONGRESS

U.S. House of Representatives

COMMITTEE ON ETHICS

1015 Longworth House Office Building
Washington, D.C. 20515–6328
Telephone: (202) 225–7103
Facsimile: (202) 225–7392

November 14, 2019

MEMORANDUM FOR ALL MEMBERS, OFFICERS, AND EMPLOYEES

FROM: Committee on Ethics
Theodore E. Deutch, Chairman
Kenny Marchant, Ranking Member

SUBJECT: Access to Classified Information and Controlled Areas

---

This memorandum serves as a reminder to all House Members, officers, and employees about the ongoing obligation to safeguard classified information and areas.

House rules require that all House Members and staff, before accessing classified information, shall execute an oath stating that he or she will not disclose any classified information received in the course of their service with the House of Representatives, except as authorized by the House of Representatives or in accordance with its rules.[1] When a Member should be aware of or is uncertain about the classification of sensitive information in their possession, they must make a good faith effort to ascertain its classification with the appropriate executive branch agency before disclosing it to the public.

To facilitate its work, the House has multiple sensitive compartmented information facilities (SCIFs) or controlled areas. Each controlled area is governed by the appropriate committee of jurisdiction or the Sergeant at Arms. However, there are basic tenets regarding access to classified information and controlled areas that all House Members and employees should adhere to.

Access to classified information and areas, even for cleared personnel, is granted on a "need to know" basis. As such, House personnel should not attempt to gain access to classified information or controlled areas unless they have a need to access the area or information. Multiple overlapping safeguards exist to protect against different types of intrusion. However, the protections rely on the cooperation of those entering a SCIF to ensure countermeasures are not compromised. Thus, portable electronic devices (PEDs) should generally not be taken into any controlled area. PEDs include, but are not limited to, cell phones, laptops, smartwatches, tablets, or any other devices capable of transmitting or receiving an electronic signal.

---

[1] House Rule 23, clause 13.

House controlled areas are accredited for operation by the intelligence community and are subject to periodic inspections to recertify their accreditation. Breaches of security protocols or unauthorized disclosures could result in the decertification of these facilities. This would significantly impair the House's ability to conduct its business.

Inadvertent breaches of security protocols or unauthorized disclosures may be handled as a matter of security by the committees of jurisdiction over the relevant classified information or controlled areas. However, attempts to gain unauthorized access to classified areas or purposeful breaches of basic security protocols may cause classified information to be improperly disclosed, and may reflect discreditably on the House as a legislative body. The Committee has jurisdiction to investigate violations of House rules, regulations, laws, or other standards of conduct, including violations of House rules regarding disclosure of classified information and other potential violations of the Code of Official Conduct.[2]

If you have any questions regarding this guidance, please feel free to contact the Committee's Office of Advice and Education at (202) 225-7103.

* * * * *

[2] House Rule 23.