

MEMORANDUM

To: Joshua Schulte, DDI/CCI/EDG/AED/RDB
From: Anthony Leonis Acting Chief, DDI/CCI/EDG/AED
Date: Monday, 18 April 2016
RE: (U//~~FOUO~~) Self-Granting Previously Revoked Admin Privileges on an Agency Computer Network

(U//~~FOUO~~) At the end of March 2016, DDI/CCI/EDG/AED/OSB staff were directed by DDI/CCI and DDI/CCI/EDG management to ensure that all AED/OSB projects were properly resourced, all AED/OSB-related development resources (to include computer network exploitation (CNE) related code libraries, development tools, etc.) were accessed and administered by the appropriate people in AED/OSB, and any projects that were not going to remain in AED/OSB be moved to the appropriate EDG branch immediately. (Note: AED/OSB is responsible for developing, among other things, ~~tools used~~ to acquire data from targeted systems)

(U//~~FOUO~~) As part of this process, on early April 2016, AED/OSB administrators of AED/OSB's CNE Code Component Libraries (known as the "OSB Libraries") removed Mr. Joshua Schulte's administrative access to the OSB Libraries following Mr. Schulte's transfer from AED/OSB to AED/RDB at the end of March 2016. In doing so, while Mr. Schulte's administrative rights to the OSB Libraries code repository were removed, Mr. Schulte maintained user-based access to the OSB Libraries code repository to permit him to access and commit code to the OSB Libraries repository through a pre-defined peer review process.

(U//~~FOUO~~) The following information was learned:

- 1) (U//~~FOUO~~) Upon learning that he was removed as an administrator of the OSB Libraries on Thursday 14 April 2016, Mr. Schulte met with OSB Developer Jeremy Weber (one of the OSB Library Admins) and Sean ~~(AED/OSB Branch Chief)~~ to discuss the situation. At the conclusion of the final discussion with Mr. Weber on Thursday 14 April 2016, Mr. Schulte reportedly remarked that he "... will eventually get access back to the libraries and that [his] access should just be enabled now ..." to Mr. Weber before Mr. Schulte left the area. Upon reading the above, Mr. Schulte remarked that his exact quote was that "... I am adding my access back, until some with authority advises me otherwise."
- 2) (U) After discussing the issue with Mr. Weber, Mr. Schulte viewed his removal from the OSB Libraries as "unauthorized."
- 3) (U//~~FOUO~~) Before the end of the day on 14 April 2016, it was discovered that Mr. Schulte had personally re-instituted his administrative access to the OSB Libraries code repository via other administrative rights Mr. Schulte possessed on EDG's DEVLAN system.

(U//~~FOUO~~) As a reminder of Agency policy, Administrative Rights are provided to trusted individuals for the sole purpose of ensuring that the right people have access to data in order to complete job-related tasks. As explained in the Agency's annual AISC trainings, (from AISC 2016, Module 2: User Accounts) "...The Agency has strict regulations and procedures for granting access to IT systems and managing user accounts. Careful management of user accounts is necessary to ensure only legitimate, trusted individuals have access.... References: AR 9-38, AR 9-25." As such, those who have rights to any system are to be reviewed, esp. as a person changes job duties. Additionally, after a change of access is reviewed and action is taken, individuals are not permitted to personally attempt and/or renew their previous authorizations to any particular system. This is a direct violation of trust, and a violation of Agency policy.

(U//~~FOUO~~) Lastly, effective 0800 on Monday 18 April, the OSB Libraries (and any associated computer network exploitation (CNE) related code libraries, development tools, etc.) will administered by designated AED/OSB personnel until further notice. Please do not attempt to restore or provide yourself administrative rights to any project and/or system for which they have been removed.

(U) The undersigned has read and understands the above.


Mr. Joshua Schulte

Working Copy - Not Official Copy