



National Security Unit Rules of Behavior for Open Source Analysis

All National Security Unit (NSU) Open Source (OS) Team users will abide by the following Rules of Behavior when conducting open source research:

1. All open source searches will be conducted in an unattributable browser, under the user's unattributable browser account as assigned by a NSU supervisor. Only in times of exigent circumstances when the unattributed browser account is not available, the NSU Supervisor may instruct the OS Team to use their attributed government equipment and browser to conduct urgent narrowly defined searches.
2. Users may only access the NSU proxy server service using government furnished equipment, and under the supervision of a designated supervisor. At no time will a user:
 - a. Create an email address or use an email address for personal or investigative purposes.
 - b. Log into any account, including but not limited to, personal or professional accounts.
 - c. Access login protected portions/pages of any website that require an email address, username, or other sign-on information.
 - d. Interact with any member of the public online. This can include, but is not limited to messaging, chatting, friending, liking, following, or subscribing to an individual.
3. Users will only conduct open source research on the subject of a submitted request and his or her associates and linked businesses.
4. In addition to the restrictions regarding engagement with individuals online, users are also prohibited from posting, creating, or sharing any content online. This includes, but is not limited to images, text, locational identifiers, or links to other web content.
5. Users will not conduct any personal business or local address searches (ex: lunch near the office) that would identify the actual location of the user while using the unattributable browser.
6. Users will not cross contaminate the unattributable browser with information that would be able to identify the DHS Network (A-LAN).
 - a. Users will not download or upload anything onto the DHS network. Only supervisors have the capability to download/upload files.
 - b. Users will not share information between the unattributable browser and the DHS Network via email, USB connection, or other methods.
 - c. Users must understand accessing a website from an attributed browser within a certain time period of an unattributed browser may reveal a relationship between the two.

This agreement will be utilized at all times when conducting open source research as an employee of the NSU. Policies set forth in this agreement were established to ensure employee compliance with federal and other business mandates, as well as abide by the code of ethics and conduct for DHS/ICE employees. It is essential that all NSU open source users operate according to policies and guidelines referenced in this agreement.

SUBJECT: NSU OS Rules of Behavior

Page 2

By signing below, I acknowledge that I have read, understand, and will comply with the National Security Unit Rules of Behavior for Open Source Analysis. Additionally, I verify that I have taken the annual ICE Social Media Privacy Training and ICE Computer Security Training. I understand that failure to comply with the Rules of Behavior could result in verbal or written warning, removal of system access, reassignment to other duties, criminal or civil prosecution, or termination.

Signature and date

Supervisor's signature and date

FOR OFFICIAL USE ONLY

2020-ICLI-00023 1314