Department of Homeland Security
NPPD Countering Foreign Influence Operations Task Force
Operational Use of Social Media Rules of Behavior

The following rules of behavior apply to National Protection and Programs Directorate (NPPD) employees, supporting the Countering Foreign Interference Operations Task Force (CFITF), with access to social media sites and the public internet for the purposes of enhancing situational awareness of foreign interference operations.

These rules of behavior are separate and apart from those rules of behavior which cover accessing social media sites and the public internet for the purpose of communications and outreach with the public.

Social Media Access

- I understand that all activities of accessing restricted internet sites or access to social media sites will be conducted in accordance with applicable law and DHS guidance.
- I understand that my access to social media under these specific rules of behavior does not include conducting communications and outreach with the public.
- I will only access those sites for which I require access to enhance situational awareness of foreign interference operations as authorized by statute, executive order, regulation, or policy. I will not attempt to access sites or perform actions I am not authorized to access or perform.
- I understand that I must complete all required role-based privacy training prior to receiving access to social media sites and that I will complete annual refresher training as long as access is still needed.
- I understand that my access requirements will be reviewed on an annual basis and that my access can be terminated at any time if it is no longer needed due to a change in official duties, if I am no longer authorized to conduct situational awareness activities, if I am under suspension due to conduct, if I separate from DHS, or if I misuse my access.
- I have read and reviewed DHS/ALL/PIA-031 ("Social Networking Interactions and Applications"), DHS/ALL/PIA-036 ("Use of Unidirectional Social Media Applications").

Operational Use of Social Media and the Public Internet

- I will only use the keywords and hash-tags associated with specific foreign interference operations, and will not conduct further investigation into other accounts or using other hash-tags or keywords.
- I will use only government-issued equipment, government accounts and government email addresses when engaging in the operational use of social media and the public internet on behalf of NPPD.
- I will not use government resources to foster commercial interests or individual profit.
- I will log off of or otherwise restrict access to any social media session when I am not personally attending to it.
- I will only use online screen names or identities that indicate an official DHS or NPPD affiliation.
- I will not engage in unofficial or personal use of social media on government equipment or use any account created on behalf of the furtherance of the NPPD mission for unofficial purposes.

Data Protection

- I will not access information that is not publicly available.
- I will not interact with individuals who posted the information. If there is a specific and clearly articulated operational necessity to interact with individuals who posted the information, I will consult my DHS supervisor, the DHS/NPPD Office of Privacy and the Office of General Counsel for guidance.

- I will not intentionally collect PII, unless that PII is necessary to understanding a foreign interference threat to critical infrastructure.
- I will not access or post classified or otherwise protected information using social media or the public internet (e.g., WikiLeaks, Pastebin, etc).
- I will document my operational use of social media, including date, site(s) accessed, information collected, and how it was used in the same manner that DHS would document information collected during normal situational awareness activities. PII will not be included any NPPD documentation.
- I will delete all raw data after 30 days.

Incident Reporting

- I will promptly report suspected or confirmed IT security incidents (e.g., compromise of usernames and passwords or infection with malware, trojans, or key logging software), and per the DHS Handbook for Safeguarding Sensitive PII and the Privacy Incident Handling Guide (PIHG), report any privacy incidents (e.g., loss or compromise of sensitive PII) to the DHS IT Help Desk at 1-800-250-7911 and my supervisor.

Accountability

- I understand that I have no expectation of privacy while using government IT systems or any accounts created on behalf of the furtherance of the NPPD mission.
- I understand that I will be held accountable for my actions while accessing and using government IT systems and social media sites and may face disciplinary action and/or criminal or civil prosecution for misuse. Additionally, misuse may lead to removal from position and/or termination.
- I understand that I am receiving access to social media for enhancing situational awareness of foreign interference operations.

Acknowledgment Statement

I acknowledge that I have read the rules of behavior; I understand them, and I will comply with them. I understand that failure to comply with these rules could result in verbal or written warning, removal of access to social media on behalf of NPPD, reassignment to other duties, criminal or civil prosecution, or termination.

Participating in the DHS Operational Use of Social Media Training is required and serves as acknowledgement and acceptance of these Rules of Behavior.