

UNCLASSIFIED

(U)NRO on Facebook and Twitter!

10/24/2014

DID YOU KNOW

The NRO Director has approved the release of an NRO Facebook page. The Office of Congressional and Public Affairs (OCPA) will be responsible for all information uploaded and shared onto the NRO page. All information posted will be unclassified and will have had prior vetting by the Information Review and Release Group (IRRG).

This effort is in response to the White House Memorandum regarding Transparency and Open Government. By establishing an NRO Facebook page it will enable a current communication channel to reinforce the public awareness about the unique role NRO has within the IC. The NRO Directive 110-6, Public Affairs Social Media Use, has been coordinated and approved throughout the Directorates and Offices (D's & O's).

NRO personnel are advised to refrain from 'friending' or 'liking' the NRO Facebook page or any other social media outlet within the IC, as it is an Operations Security (OPSEC) issue. If you were to 'friend' or 'like' the NRO site you are providing a connection to not only the NRO but with the IC. It is extremely easy for adversarial characters to target openly associated names. This is what would create the OPSEC issue. Those in a cover status should follow all instructions from the office.

(b)(3)

It is important to understand the many aspects of how the Foreign Intelligence Services (FIS) target people within the IC and how to mitigate their advances. NRO personnel are targets for FIS for no other reason than you have access to intelligence information. Understanding the fact that you control your personal information and what you choose to share is the first step to protecting it. Being familiar with all privacy settings and utilizing them for each of your social sites is important. Maintaining a strong security network at home is essential; update your anti-virus and antispyware protection, keep your firewall turned on, and update your system software regularly. Most importantly understand that once you have an internet presence, the information you post tells a story; will yours make you more of a target for elicitation?

Remain vigilant, protect your information, and talk with your Program Security Officer (PSO) if you have any questions.

UNCLASSIFIED