Ministry of Defence

Industry Security Notice

Number 2022/06

National Security Vetting and Social Networking Sites

Action for Company Security Controllers

1. Security Controllers must ensure the following instructions are communicated to all personnel within their organisation who hold a National Security Vetting (NSV) clearance.

Instructions for NSV Clearance Holders

2. If individuals use social networking sites/apps and advertise their security clearance (e.g. the level of clearance they hold), they are putting their self, colleagues and national security at risk. Individuals must remove these details from their social networking profiles immediately.

3. All National Security Vetting (NSV) clearance holders have an obligation to exercise discretion and good judgement as an on-going requirement of holding their clearance. Failure to adhere to this requirement will result in the vetting clearance being reviewed to determine if they are still suitable to hold it and this could jeopardise their employment.

4. A recent campaign by the Centre for the Protection of National Infrastructure highlights that engaging with the wrong person could damage someone's career, their life, and their colleagues' careers, along with the interests of UK national security and prosperity.

5. **NSV Clearance Holders Must:**

- **Never advertise their security clearance.** Alert colleagues if you spot their social networking profile does this and remind them to remove the reference immediately.

- **Do not overshare,** and think carefully about the personal information you put on social networking accounts. If you tell people where you went to school, university, interests, and hobbies, they can use this as a hook to get into your life.

- **Remember you have signed the Official Secrets Act** – do not disclose any details about your classified work online or with casual acquaintances. Apply good judgement and discretion as to who you disclose your job title or your work location to.

- **Always be alert to requests for information on/from third parties**. You could be used to provide information on others. Seemingly small pieces of information gleaned from multiple sources can be built up to a surprisingly rich picture e.g. phishing attempts or identity theft. It is strongly recommended that you do not accept social networking contact requests from people you do not know.

- **Trust your instincts, do the right thing, and report it to security.** Report any suspected hostile approach (no matter how trivial it might seem) to your Security Controller.

Validity / Expiry Date

6. This ISN will expire when superseded or withdrawn.

MOD Point of Contact Details

7. The point of contact in respect of this ISN is:

DES PSyA
Ministry of Defence
email: despsya-pers-sy@mod.gov.uk (Multiuser) or