Counterintelligence Awareness for Government Employees and Contractors

FBI GUIDANCE TO GOVERNMENT EMPLOYEES AND CONTRACTORS

All US Government employees should be aware of potential counterintelligence concerns arising from the recent compromise of US Office of Personnel Management (OPM) data. The data compromised may include personally identifiable information about US Government employees, such as names, addresses, phone numbers, e-mail accounts, and records related to personnel actions. Foreign governments, particularly foreign intelligence and security services, can use compromised personal information to target and collect additional information about/from US Government employees and their relatives and associates. Targeting can include attempts by foreign government actors to compromise personal electronic devices such as smartphones and computers. ■

GENERAL GUIDANCE

All affected individuals should understand their US Government affiliation is possibly known to foreign governments and stay vigilant to recognize any indications of targeting.

- Be wary of unsolicited attempts by unknown individuals/groups to make contact via e-mails, telephone calls, social media interactions, and personal encounters.
- Take care in providing personally identifiable information (e.g., Social Security number, dates of birth, account information, etc.) to sources who are not trusted and verified.
- Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at www.ic3.gov.

- Be careful with personal and work-related information you transmit, particularly via telephone and the Internet. Metadata in electronic files and photographs contains a great deal of identifiable information, including file creation timestamps and location information.

- Be alert to suspicious activities related to personal electronic devices, such as Internet spam messages from unknown senders and excessive or out-of-cycle software downloads/updates. Be careful about opening e-mails and clicking on links within e-mails from unknown senders.

- Be careful transmitting financial account information, and periodically check your credit history.

- Report suspicious events and contacts experienced by your relatives and associates, particularly those individuals identified in OPM personnel records. Consider notifying and discussing this event with any affected relatives and associates.

- Report suspicious activity to your employer and/or the FBI.

TRAVEL OVERSEAS

When traveling overseas, all affected individuals should assume their US Government affiliation is likely known to the foreign governments of the countries they are visiting. Consequently, affected individuals should remain particularly vigilant when abroad.

- Do not bring or discuss anything sensitive while overseas. Safeguard personal documents, such as your driver's license, passport, and credit cards.

- Be particularly alert to suspicious activities or compromises related to personal electronic devices while overseas, and consider leaving personal electronic devices at home.

- Avoid risky or embarrassing behavior overseas. Foreign intelligence and security services can exploit vulnerabilities or misconduct overseas to either recruit or coerce you into disclosing sensitive information.

- Know the locations and contact information for US embassies, consulates, and other diplomatic establishments for any issues and/or emergencies. ■

PROTECT YOURSELF AGAINST INTRUSION

To protect yourself and your family, the FBI urges all affected individuals to exercise caution and remain vigilant to any events appearing out of the ordinary or suspicious.

If you believe you have observed activity related to this compromise or suspect you are being targeted, report your concern through the appropriate organizational channels (supervisor, security officer, etc.) for your employer and/or directly to your local FBI field office. ■

Please contact OPM at media@opm.gov if you are contacted by the Media.
FBI employees can reach out to the FBI National Press Office at NPO@ic.fbi.gov.