United States Senate
COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS
WASHINGTON, DC 20510–6300

February 9, 2026

Howard Langsam
Chief Executive Officer
OPEXUS
1101 17th St NW #1200
Washington, DC 20036

Dear Mr. Langsam:

Securing access to critical information technology (IT) is essential to ensure that sensitive government and consumer information is not misused. At a time when cybersecurity incidents are only increasing in frequency, it is important that those who have access to this data take their responsibility to protect public and private stakeholders seriously.

The recent cybersecurity breach involving OPEXUS raises questions about the company's commitment to robust cyber practices. OPEXUS offers a number of products for state, local, and federal agencies, including tools to manage Freedom of Information Act (FOIA) requests, workflow management, and agency audit and investigation activities. OPEXUS explicitly states that "security should be at the forefront of everything we do."[1]

Contrary to this stated commitment, OPEXUS recently employed two individuals who previously pleaded guilty and received prison sentences for hacking federal agencies, specifically the Department of State.[2] Despite their criminal records, OPEXUS was unaware of this information when the two individuals were hired in 2023 and 2024, respectively, although OPEXUS claims that both individuals underwent background checks prior to their employment.[3]

After learning about their criminal history in February 2025, the two individuals were terminated.[4] However, prior to losing access to OPEXUS' systems, these individuals allegedly destroyed and exfiltrated a number of government documents, including those belonging to the Equal

[1] *Federal Product Offerings*, OPEXUS (Jan. 21, 2026), https://www.opexustech.com/federal-solutions/.
[2] Jason Leopold, *The Case of the 'Lost' FOIA Requests*, Bloomberg (May 21, 2025), https://www.bloomberg.com/news/newsletters/2025-05-21/how-2-hackers-erased-hundreds-of-foia-requests.
[3] Matt Kapko, *Opexus claims background checks missed red flags on twins accused of insider breach*, Cyberscoop (Dec. 15, 2025), https://cyberscoop.com/opexus-background-checks-insider-attack-muneeb-sohaib-akhter/.
[4] Matt Kapko, *Twins with hacking history charged in insider data breach affecting multiple federal agencies*, Cyberscoop (Dec. 3, 2025), https://cyberscoop.com/muneeb-sohaib-akhter-government-contractors-insider-attack/.

Employment Opportunity Commission (EEOC).[5] This incident resulted in several federal agencies temporarily losing access to its FOIA systems.[6]

These developments raise significant concerns about OPEXUS' internal processes to safeguard sensitive information. To that end, I ask that you answer the following questions by **February 24, 2026**.

1. On February 18, 2025, OPEXUS terminated the two employees in question.[7] However, the two employees still had access to OPEXUS' internal systems and allegedly deleted 96 government databases and exfiltrated approximately 1,800 files belonging to the EEOC.[8]
   a. Why did OPEXUS not immediately terminate the two employees' access to its internal systems?
   b. What safeguards did OPEXUS have in place to limit the deletion or exfiltration of such data?
   c. Was OPEXUS able to recover the databases allegedly deleted by the two employees?
   d. OPEXUS states that it works with many government agencies and supports 78% of agencies in processing FOIA requests. Has OPEXUS identified what government agencies were impacted by the cybersecurity incident? If so, please provide a list of impacted agencies.
   e. How is OPEXUS working with federal agencies to identify what information was inappropriately accessed and to remediate any security risks?

2. OPEXUS is currently certified under the Federal Risk and Authorization Management Program (FedRAMP). As part of that certification, contractors must have personnel screening policies in place.[9]
   a. How does OPEXUS screen prospective employees prior to employment?
   b. Does OPEXUS conduct audits or additional screening of current employees?

3. OPEXUS has previously stated that the two terminated employees had undergone background checks prior their employment, but that "additional diligence should have been applied."
   a. What lapses to OPEXUS' pre-employment processes has it identified that led to the two terminated employees prior criminal convictions being missed?

---

[5] *Id*.
[6] *See note 2*.
[7] *See note 4*.
[8] *Id*.
[9] *What does FedRAMP require for personnel screening requirements from cloud service providers (CSPs)?*, FedRAMP (Sept. 4, 2024), https://help.fedramp.gov/hc/en-us/articles/27707270509339-What-does-FedRAMP-require-for-personnel-screening-requirements-from-cloud-service-providers-CSPs.

b. What remedial steps has OPEXUS implemented to its pre-employment processes?

4. Since 2020, how many employees or former employees has OPEXUS terminated due to potential security vulnerabilities? If applicable, please provide the number of terminations by year, including the potential vulnerability OPEXUS identified.

5. OPEXUS' negligence caused some Americans' personally identifiable information to be exposed.
    a. Has OPEXUS provided credit monitoring at no cost to individuals impacted by the cybersecurity incident? If not, will OPEXUS commit to doing so?
    b. Has OPEXUS agreed to indemnify against any financial losses as a result of the cybersecurity incident? If not, will OPEXUS commit to doing so?

Sincerely,

Bill Cassidy, M.D.

Bill Cassidy, M.D.
Chairman
U.S. Senate Committee on Health,
Education, Labor, and Pensions