2026 DSAC Annual Survey

Instructions

Thank you for participating in the 2026 Domestic Security Alliance Council (DSAC) Annual Survey. Your feedback is vital in helping the DSAC Program Office assess program effectiveness and develop future trainings to align with your experiences and needs.

This survey will take approximately 10 minutes to complete. If you have any questions, please contact us at DSAC@fbi.gov. We appreciate your time and input!

Select "**Next**" to move to the next section.

Section 1: Current Threat Landscape

Objective: Understand their perception of relevant challenges and knowledge gaps.

1. **What do you see as the most significant threats or challenges impacting your field right now?** *(Open-ended)*

2. **Do you feel equipped to address these challenges in your role?** *(Likert scale: Strongly Agree to Strongly Disagree)*

3. **What areas of the current threat landscape would you like additional resources for?** *(Multiple choice with an "Other" option for additional input.)*

    - Cybersecurity Threats
        - **Ransomware Attacks –** Latest trends, prevention strategies, and incident response best practices.
        - **Phishing and Social Engineering –** Advanced tactics attackers use and methods for mitigating risks, and remote intrusions.
        - **Insider Threats –** Strategies to detect and prevent malicious or negligent insider activity such as unauthorized Access to Data, Data Exfiltration, Credential Misuse, Sabotage, or Unintentional Actions.
        - **Supply Chain Attacks –** Understanding risks from third-party vendors and securing the software supply chain.
    - Physical Security Threats

- **Active Shooter or Workplace Violence Preparedness** – Training and protocols to minimize risks and respond effectively.
- **Executive Protection –** essential strategies, risk assessment, and real-world tactics to ensure the safety of high-profile individuals in dynamic threat environments.
- **Supply Chain Attacks –** Understanding risks from third-party vendors and securing the physical supply chain.
- **Insider Threats –** Strategies to detect and prevent malicious or negligent insider activity, such as Unauthorized Facility Access, Theft of Physical Assets, Espionage, Sabotage, or Tailgating and Access Abuse.
- **Threat Assessment and Behavioral Analysis –** Identifying warning signs of escalating threats, recognizing behavioral patterns, understanding risk levels and potential for violence.
- **Situational Awareness and Surveillance Detection –** Techniques to detect and counter surveillance, identifying suspicious activities and persons, body language and environmental scanning.
- **Violent Crime-** acts involving the use or threat of force, such as assault, robbery, homicide, and domestic violence, violent protests, etc., that occur within a business environment and impact employee safety and workplace culture.

- Global Threats
  - **Geopolitical Risks –** Impact of conflicts, sanctions, or tensions on organizational operations and cybersecurity.
  - **Terrorism and Extremism –** Current trends and how they may affect business operations or employees.
- Emerging Threats
  - **AI-Powered Cyber Attacks –** Exploitation of AI by adversaries, such as deepfakes and automated phishing.
  - **Quantum Computing Implications –** Potential impact on encryption and long-term data security.
  - **Connectivity & Connected Devices–** Risks from connected devices in both consumer and industrial environments, including the increased connectivity and speed of 5G networks.
- Industry-Specific Threats
  - **Critical Infrastructure Risks –** Threats to energy, water, transportation, and other essential services.
  - **Healthcare Cybersecurity –** Risks to patient data and operational technology in hospitals.
  - **Financial Fraud and Cybercrime –** Latest methods in financial scams, wire fraud, and ATM hacking.

4. **What type of additional resources would you find most helpful for the topics you identified as important?** *(Multiple choice with an "Other" option for additional input.)*

- Virtual webinars
- In-person town halls or workshops
- Intelligence products (including LIRs) or newsletters
- Conferences
- Other (please specify)

Section 2: Feedback on Engagement and Programming

Objective: Assess the relevance and impact of the program's offerings, and the office's interactions and program engagement.

5. **What type of communication works best for the DSAC Program Office and your DSAC membership, for collaboration?** *(Open-ended)*

6. **How satisfied are you with the DSAC Program Office's programming for emerging threats (e.g., CTD call, Executive Protection Webinar)?** *(Likert scale)*

7. **How satisfied are you with the DSAC Program Office's long-standing programming for annual events (e.g., DSEA, GDSEA, Annual)?** *(Likert scale)*

8. **Do you feel the programming helps improve your skills or understanding of key issues?** *(Yes/No with optional explanation.)*

9. **What's working well for communication and collaboration, with your local field office and the PSC(s)?** *(Open-ended)*

10. **How would you rate DSAC program engagement at your local field office?** *(Likert scale with an optional comment box.)*

11. **How can the DSAC Program Office better support your DSAC membership, through the Program Office, the local field office and/or the PSC(s)?** *(Open-ended)*

12. **Do you use the DSAC Portal to access intelligence products? If so, how frequently do you or your team log in? (open-ended)**

Section 3: Event Hosting

Objective: Gauge willingness and capacity for hosting.

13. **Would your office be willing to host an event or FBI training?** *(Yes/No)*

14. **If yes, what is the capacity your office can accommodate for an event?** *(Numeric or dropdown options: 20-50, 50-100, 100-250, >250)*

15. **Please provide a POC to coordinate scheduling:** *(Open-ended)*

16. ***Would you or someone from your organization be willing to present at upcoming DSAC events?***

Survey Closing

17. **Optional: Would you like to provide your contact information?** *(Open-ended)*

18. **Optional: Would you like to provide additional comments or suggestions?** *(Open-ended)*

19. **Would you like us to follow up with you? If so, please provide your name and contact information.**