How Your Information Will Be Used

We take your privacy seriously. By registering for SOF Week 2026, you agree that your data will be used for event-related purposes and managed securely as described below.

Data Controllers and Use

SOF Week is jointly sponsored by **U.S. Special Operations Command (USSOCOM)** and the **Global SOF Foundation (GSOF)**. GSOF contracts **MCI Group** to execute event services, including vetting of registrants. **GSOF** and **MCI Group** act as Joint Independent Data Controllers. This means your data will be shared with both parties and used to manage event logistics and contact you about this event and its future editions, based on our legitimate interests. **Cvent**, our registration vendor, acts as the assigned Data Processor, managing your data securely on our behalf. Your information will always be used in accordance with the [MCI Privacy Policy](#) and the [GSOF Privacy Policy](#). All registration, profile, and behavioral data remain wholly owned by MCI and GSOF.

ID and Photo Verification

We collect specific documents and images solely for the purpose of event verification.

Your **Identification Document (ID Data)** will only be used for verification. It is stored securely as an encrypted binary image and will be **permanently deleted** from all databases within **30 days** of the event's conclusion. Your **Headshot Photo** will be associated with your SOF Week mobile app profile. You can modify it after logging in, and your photo will **not** be visible to other attendees if you choose not to be included in the Attendee Listing.

USSOCOM Enterprise Personnel will not be asked to submit ID or Photo Verification.

Data Retention and Deletion

All data collected for **USSOCOM Enterprise Personnel** will be **obfuscated** within **30 days** of the event's conclusion. As noted above, all **ID Data** will be deleted within 30 days of the event.

Data Security and Standards

Your data is submitted and stored securely on the **Cvent web-based platform**. Cvent uses a secure AWS environment (East Coast region, backed up in a West Coast Disaster Recovery site). Access to your data is restricted to authorized staff, who use multi-factor authentication. All access is logged and reviewed through a Security Information and Event Management (SIEM)

tool. All data is encrypted at the disk level. Sensitive PII (such as SSN, passport numbers, and credit card numbers) is also protected by **field-level encryption**. Cvent is certified on **PCI DSS Level 1** and **SOC2 Type II**, adhering to **NIST Cyber Security Standards** and international standards like **GDPR**.