

**Security Agreement for
Government Sponsored Meeting
Between**

NexTech Solutions, LLC

6701 South Dale Mabry Highway Tampa FL 33611

813.566.1402

shelton.richards@nextechsol.com

Government Sponsor Name

Government Sponsor Host Organization
(ex: SPACECOM J66)

Government Sponsor Address

Government Sponsor POC Email Address

Signed on behalf of *NexTech Solutions, LLC*
by *(Shelton Richards FSO)*

Signed on behalf of

(government sponsor host organization)

(government sponsor name and title)

Purpose of the Security Agreement:

*Provide an **unclassified** narrative explaining:*

- *The purpose of the meeting* _____
- *The dates of the meeting* _____
- *The classification level of the meeting* _____
- *The precise location of the meeting and room number* _____
- *The entities in attendance* _____
- *Classified equipment* _____

Classified equipment will not be authorized at the NTS facility if the required documents are attached to the agreement. Refer to section VI

- *If applicable: Equipment Test date* _____
To test equipment at NTS, the items in section VI will need to be submitted prior to the test date.
- *If applicable: A list of foreign representatives (including their nationality, name, organizational affiliation)*

Security Arrangements:

I. Announcements. Approval of the USG sponsor will be obtained for all announcements of the meeting.

(A) Announcements will be unclassified and will be limited to a general description of topics expected to be presented, names of speakers, and administrative instructions for requesting invitations or participation.

(B) Classified presentations will not be solicited in the announcement.

(C) The announcement will specify that security clearances and justification to attend classified sessions are to be forwarded to the authorizing agency or its designee.

(D) *(If applicable)* Invitations to foreign persons will be sent by the authorizing USG agency.

II. Clearance and need-to-know. All persons in attendance at classified sessions will possess the requisite clearance and need-to-know for the information to be disclosed.

(A) Need-to-know will be determined by the authorizing agency or its designee based on the justification provided.

(B) Attendance will be authorized only to those persons whose security clearance and justification for attendance have been verified by the security officer of the organization represented.

(C) The names of all authorized attendees or participants must appear on an access list with entry permitted to the classified session only after verification of the attendee's identity based on presentation of official photographic identification such as a passport, contractor or USG identification card. It is requested that the meeting access list is submitted 72 hours prior to the meeting.

III. Presentations. Classified information must be authorized for disclosure in advance by the USG agency having jurisdiction over the information to be presented.

(A) Individuals making presentations at meetings will provide sufficient classification guidance to enable attendees to identify what information is classified and the level of classification.

(B) Classified presentations will be delivered orally or visually.

(C) Copies of classified presentation materials will not be distributed at the classified meeting, and any classified notes taken during classified presentations will be marked, safeguarded, and transmitted as required per 32 CFR § 117.

IV. Physical security. The physical security measures for the classified sessions will provide for control of, access to, and dissemination of, the classified information to be presented and will provide for secure storage capability, if necessary. The sponsor will ensure that the space used to host the classified meeting:

(A) Will not contain Bluetooth, wireless, or Wi-Fi enabled devices.

(B) Will not contain cameras or recording devices.

(C) Will not permit the introduction of portable electronic devices (e.g. Smartphones, Fitbits, Smartwatches, etc.) within the space.

(D) Will utilize all pertinent security measures (e.g., white noise, perimeter boundaries, signage, opaque windows, limit ingress/egress access points, etc.) necessary to preclude an unauthorized disclosure of national security information.

V. Disclosure authority at meetings. Authority to disclose classified information at meetings, whether disclosure is by officials of industry or USG, must be granted by the USG agency or activity that has classification jurisdiction over the information to be disclosed. Each contractor that desires to disclose classified information at a meeting is responsible for requesting and obtaining disclosure approvals. Associations are not responsible for ensuring that classified presentations and papers of other organizations have been approved for disclosure. A contractor desiring to disclose classified information at a meeting will:

(A) Obtain prior written authorization for each proposed disclosure of classified information from the USG agency having jurisdiction over the information involved.

(B) Furnish a copy of the disclosure authorization to the USG agency sponsoring the meeting.

VI. Information System Security. The government sponsor may not physically or electronically connect to any unclassified or classified information processing system or peripheral (e.g., printer, copier, scanner, etc.) owned by *NexTech Solutions, LLC*.

Prior to hosting the government sponsored meeting the contractor shall provide their cognizant security agency (DCSA) representatives with:

i. A written list of classified devices the USG sponsor will bring to the contractor facility.
[*Commercial Solutions for Classified (CSfC), SIPR 'flyaway' kits, etc. are not authorized in contractor facilities].

ii. A current Authority to Operate (ATO) for each USG system.

iii. A mobile mission plan for the USG systems.

VI. Government Certification. By signing the above, the government representative certifies that he or she is authorized to enter into this agreement on behalf of _____ and accepts responsibility for complying with the security requirements delineated in the agreement.

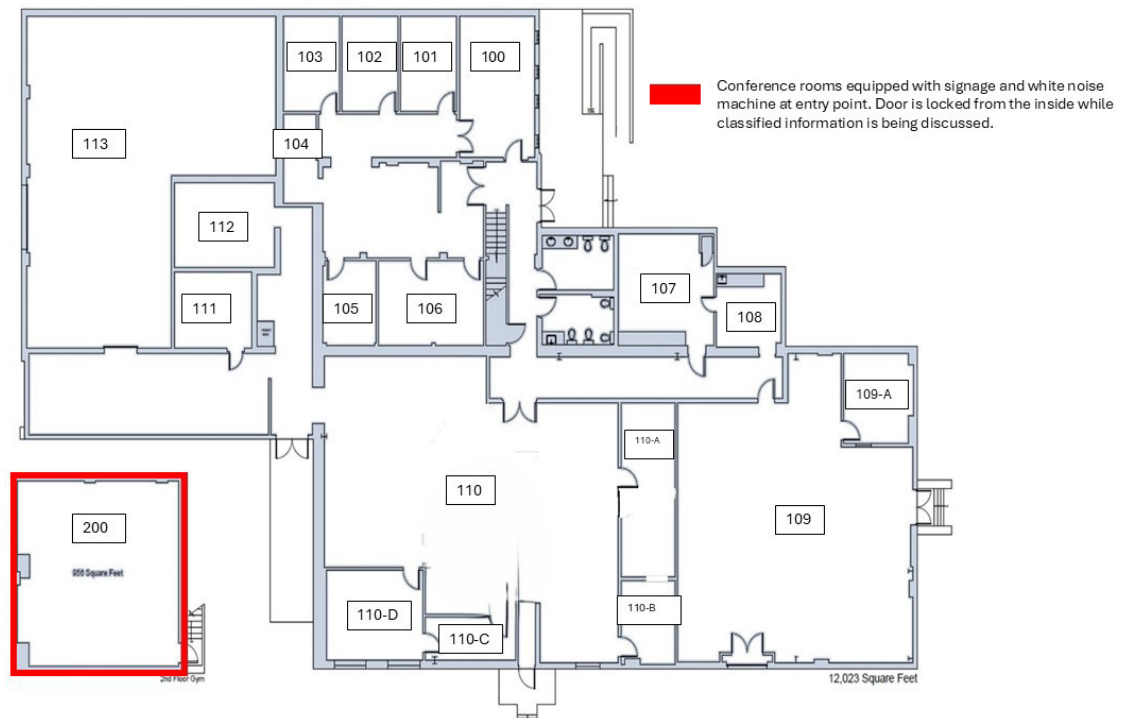
VII. Security Incidents. By signing the above, both parties agree to immediately report acts of non-compliance with this agreement concurrently to DCSA and the USG sponsors' security point of contact. Any loss, compromise, or suspected compromise of national security information shall be immediately reported to DCSA IAW 32 CFR § 117.8(d).

Attachments:

- A. Diagram of the Pinewood facility utilized to host the event
 - A.1 Diagram of the Ybor facility utilized to host the event
- B. Sample of Event Badge/ID
- C. DD 254 associated with event (if applicable)
- D. List of Foreign Representatives (if applicable)
- E. List of Classified Devices (if applicable)
- F. Current ATO for each USG system (if applicable)
- G. Mobile Mission Plan (if applicable)
- H. Authorization to Disclose Classified Information (if applicable)

Attachment A.

Attachment A.1

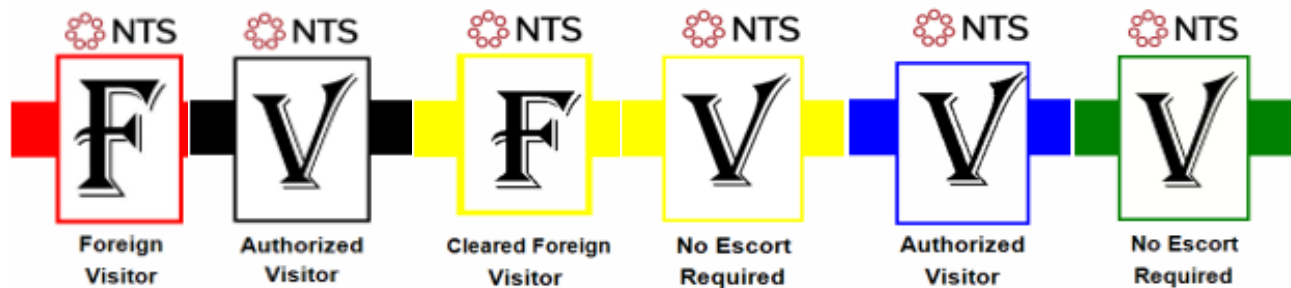


Attachment B.

NTS Badges

Badges below are issued to all visiting personnel in reference to their citizenship status/clearance level.

All foreign nationals required to access classified information are vetted through the owning USG agency of information being presented.



Green indicates TOP SECRET/SCI

Blue indicates TOP SECRET

Yellow indicates SECRET

Black/Red indicates NO CLEARANCE or NO CLEARANCE ON FILE