Certification of Security Clearances to the University of Maryland Center for Advanced Study of Language

The University of Maryland Center for Advanced Study of Language (CASL) is a Sensitive Compartmented Information Facility (SCIF).

The CASL CONFIRM reader now accepts the following blue IC and green contractor badges.

**All others should submit their clearances to CASL at least 7 business days prior to event**

Clearances for all visitors to the CASL SCIF must be certified in writing to the Director of Security. This is a requirement by DIRNSA. Clearances should be certified for a one (1) year period if multiple visits are anticipated.

**These scenarios can be used to determine the required actions by proposed visitors to the CASL SCIF:**

a. **For organizations outside the IC agencies listed above,**

   - The supporting Special Security Office (SSO) must certify each individual’s clearance electronically to **NSA/CSS/Q123 PASS TO UMD/CASL MARK TISE**. Q123 will prepare the appropriate letter and fax it to CASL. Note that SCI clearances must be sent via electronic message. NSA will not accept SCI accesses via fax. **Please allow 7 working days for all actions to occur.**
   - The supporting SSO must certify each individual’s clearance via JPAS to SMO Code OUB92 – Center for Advanced Study of Language, Mark Tise.

b. **Contractors not possessing a green contractors badge may have their company SSO complete a visit certification to the CASL Director of Security, fax number 301.226.8943. Contractors for other government agencies must follow the instructions in subparagraph a, supra.**

**CASL Security Team Contact Information:**

**Assistant Director of Security/ACSSO**

Aye J. Vines  
Email: avines@casl.umd.edu  
Phone: 301.226.8937  
Fax: 301.226.8943

**Security Coordinator/ACSSO**

Zanaki Renibe  
Email: zrenibe@casl.umd.edu  
Phone: 301.226.9020  
Fax: 301.226.8943
Prohibited Items List

Policies prohibit the following items in controlled spaces:

1. Firearms and/or ammunition.
2. Explosives, incendiary substances, radioactive material, flammable liquids, solids, gasses or other hazardous materials.
3. Two-way pagers.
5. iPods, MP3 players and other digital audio players.
6. AM/FM Radios.
7. Personally owned two-way radio transmittal (CB, Wi-Fi, HAM, etc.)
8. Personally owned test, measurement and diagnostic equipment.
9. Personally owned photographic and recording equipment (audio, video, optical) and associated information storage media.
10. Personally owned computers (laptops, notebooks, PDAs, C-Pens, etc.) and associated information storage media.
11. Personally owned portable drives to include flash drives, memory sticks or any other like device.

Note:

- Burned CDs are allowed in the SCIF for work purposes only (i.e. briefings) and must be scanned at the Self-Scanning Virus Station prior to its introduction to the unclassified computer system.
- Otherwise, only commercially produced CD/DVDs may be introduced into the SCIF.