



# DEFENSE SECURITY SERVICE

## FOCI Newsletter

Issue 2

April 19, 2001

### WELCOME NEW OUTSIDE DIRECTORS AND PROXY HOLDERS

We would like to take this opportunity to welcome Outside Directors, Proxy Holders and Trustees that have joined us since the last FOCI Conference held September 27, 2000. We look forward to working with you in the National Industrial Security Program.

### ANNUAL FOCI CONFERENCE

The Defense Security Service (DSS) Seventh Annual FOCI Conference is scheduled September 25, 2001, at the Central Intelligence Agency Conference Center, Langley, Virginia. The Conference is designed for individuals who serve as Outside Directors, Proxy Holders or Trustees at U.S. foreign-owned cleared government firms. We understand that scheduling conflicts may not allow attendance by all Outside Directors, Proxy Holders or Trustees from each firm. However, we encourage attendance by at least one of the individuals from each company cleared through a FOCI arrangement. Additional information will be provided to you within the next couple of months. We look forward to your participation.

### EXPIRATION OF AGREEMENTS

Agreements entered into by the Department of Defense (DoD) with U.S. firms operating under FOCI have an expiration date of ten years from the effective date of the Agreement. The effective date is the date in which an official of the DSS executes the Agreement on behalf of the DoD. If your firm's Agreement is due to expire this year, please advise the firm's Facility Security Officer to contact the local DSS, Industrial Security Representative (IS Rep) to coordinate renewal of the Agreement. Since new language has been incorporated into our draft agreement within the past two years, execution of a new Agreement versus an amendment to the existing agreement is required.

---

### INSIDE THIS ISSUE

- 1 Welcome
- 2 Annual FOCI Conference
- 3 Expiration of Agreements
- 4 New Industrial Security Letters
- 5 DISCO Relocation
- 6 Monitoring Electronic Communications
- 7 DSS FOCI Points of Contact

## ISSUANCE OF NEW INDUSTRIAL SECURITY LETTERS

Industrial Security Letters (ISL 01L-1 and ISL 01L-2) approved by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD (C3I)), are now available on the DSS website: ([www.dss.mil](http://www.dss.mil)). Firms under the National Industrial Security Program will also be receiving a hardcopy in the mail.

ISL 01L-1 is dedicated to interpreting and clarifying guidance in Change 2, Chapter 8, Automated Information Systems, National Industrial Security Program Operating Manual (NISPOM).

ISL 01L-2 contains articles on the following topics: DoD Security Clearance/Access Investigative Priorities, Defense Industrial Security Clearance Office's (DISCOs) Relocation, Electronic Personnel Security Questionnaire (EPSQ) Technical Help Desk, Reciprocity of Intrusion Detection Systems, Establishment of the Industrial Base Clearance Requirements Office (CRO) by DSS, Defense Central Index of Investigations (DCII) Systems Access Center, Adverse Information as it Relates to the Office of Secretary of Defense (OSD) Reinstatements and Conversion Waiver, and Suspicious Contact Reports.

## DEFENSE INDUSTRIAL SECURITY CLEARANCE OFFICE (DISCO)

Effective March 12, 2001 DISCO completed their move to a new location. The new mailing address is:

Defense Security Service  
Defense Industrial Security Clearance  
Office  
2780 Airport Drive, Suite 400  
Columbus, Ohio 43219-2268

The phone number for Customer Service (general inquiries) has not changed. It is 888-282-7682.

## MONITORING ELECTRONIC COMMUNICATIONS

In the past two years, FOCI mitigation agreements with foreign owned firms have included a clause which sets forth a requirement for oversight of electronic communications. Specific details of how this is to be accomplished at each firm are not specified in the agreement. Such details are to be formulated by the companies themselves to assure that security goals are met within their operational environment. Tools are available to help accomplish this task.

There is no "one size fits all" solution to controlling and monitoring electronic communications. Each environment will require a review of what's currently in use at the facility plus research into products, services, and procedures. Periodic evaluation of systems employed to support oversight of electronic communications should also be made to assure effectiveness and efficiency and to take advantage of new technologies.

Books and periodicals are commercially available which outline both technical and procedural steps to control and monitor electronic communications. As an example, the February 26, 2001 edition of "InfoWorld" has an article entitled "Thought Cop" which assesses software solutions for controlling and monitoring e-mail and web access. Among common features of such software mentioned in the article were content filtering, e-mail scanning with monitoring or redirection and web monitoring. Larger computer stores offer a variety of current books on these topics. In general, public libraries have limited publications in this subject area and college or university libraries may have extensive collections to support their academic programs.

Manuals for communications equipment are also a resource. A look through the manual of a fax machine at DSS headquarters disclosed several features useful for controlling or monitoring transmissions. There were PIN code options, which can be used to control users, options for (cont'd page 3)

(cont'd)

transmission restrictions, and choices of transmission and receipt reports including images.

Phone service automated monitoring tools are limited in comparison to other media. Records of long distance calls can be reviewed for calls to the foreign shareholders or affiliates, however, phone logs kept by employees would probably provide a better record. Visit records and records of meetings can likewise be employee responsibilities.

Security education is mandatory to assure that procedures used to support the security program and the provisions of the agreement are properly implemented. In addition to the procedures themselves, training needs to cover why controls are being put into place and what the expectations of the employees should be.

Employee privacy expectations need to be addressed when proposing a system to provide oversight of electronic communications. Chapter 1, Section 3 of the National Industrial Security Program Operating Manual sets forth reporting requirements for cleared individuals and organizations and recent FOCI mitigation agreements have set standards for oversight of communications with foreign affiliates. Company policy must spell out the limitations of privacy and be communicated to each employee.

The extent of the review of electronic communications is a function of the expected volume of traffic and the tools available. Where there are limited communications a complete review may be practical. More extensive communications coupled with monitoring software might find a random or targeted sampling to be the optimal means of providing assurance that communications with the foreign affiliates are in compliance with the terms of the FOCI mitigation agreement.

Your IS Rep can provide advice and assistance in both the initial and on going phases of control of electronic communications. The IS Rep has the constraint that there is no accreditation program for computers used for unclassified work and there is no official product evaluation by DSS for most types of off-the-shelf hardware and software.

(cont'd)

Consequently, the IS Rep's role is advisory, and the final decision on what methods and components are used is up to the company. The IS Rep will review the operation of the system periodically and evaluate its operation with respect to the standard specified in the agreement.

These review techniques can also be employed by the facility to evaluate its own program. At the conclusion of the review, the IS Rep will give an overall evaluation of the system of controls and monitoring. This is an opportunity to discuss methods of improvements in the effectiveness and efficiency of the system. Electronic communications continue to change and evolve; consequently, controls can be expected to do likewise. Utilizing the talents and knowledge of employees, management, IS Reps, vendors, and security personnel is essential in maintaining the viability of a system to assure both the company and DSS that electronic communications do not disclose classified and/or export controlled information and are not used to allow the foreign owner improper influence on the performance of classified contracts.

## DSS POINTS OF CONTACT

The DSS Headquarters, FOCI Division is comprised of the following individuals who can be reached at the following telephone numbers and/or e-mail address:

Otelia Rice  
Chief, FOCI Division  
(703) 325-5292

### STAFF

Norman Johnson - (703) 325-6032  
Alton Westrick - (703) 325-5495  
Mark Nolan - (703) 325-6060  
Douglas Fontenot - (703) 325-5168  
E-mail address is: [FOCIHQ@mail.dss.mil](mailto:FOCIHQ@mail.dss.mil)

Mailing address:

Defense Security Service  
Industrial Security Program Office  
FOCI Branch (ISF)  
1340 Braddock Place  
Alexandria, VA 22314

Return Address  
Street Number and Name  
City, State 98765-4321

BULK RATE  
US POSTAGE  
PAID  
PERMIT NO.  
98765

ADDRESS CORRECTION REQUESTED

Mailing Address  
Street Number and Name  
City, State 98765-4321