CLEARED EMPLOYEE REPORTING REQUIREMENTS

As an individual who has been granted a personnel security clearance (PCL) by the U.S. Government, you are required to report the following issues to Security for investigation, resolution, and reporting to the appropriate government agency. If you have access to Special Access Programs (SAP) or Sensitive Compartmented Information (SCI), you may have reporting requirements beyond those basic requirements listed here.

Report any issues to the MSU/Office of Research & Economic Development/Facility Security Office, Neil E. Lewis, telephone (662)325-8682 or cell telephone (662)648-7265.

1. Adverse Information

Adverse information is any information that adversely reflects on the integrity or character of a cleared employee, which suggests that his/her ability to safeguard classified information may be impaired, or that his/her access to classified information clearly may not be in the interests of national security. You must report the following types of information about yourself or other employees:

- arrests or convictions for criminal offenses including drunk driving;
- financial difficulties, including bankruptcy, excessive indebtedness, and wage garnishments;
- bizarre or notorious behavior;
- alcoholism, use of illegal drugs, or abuse of legal drugs;
- emotional or psychological problems requiring treatment or hospitalization;
- affluence (wealth, acquisitions, investments) beyond known sources of income.

2. Change in Personal Status

If you have a collateral CONFIDENTIAL, SECRET, or TOP SECRET clearance, you must report:

- a change in name;
- a change in marital status (i.e., marriage or divorce);
- a change in citizenship;
- when access to classified information is no longer required due to a change in job assignments.

Note that if you have access to SAP/SAR/SCI or National Programs, you must report other changes in personal status including family deaths and births, change of address, and inheritances.

3. Representative of a Foreign Interest (RFI)

You must report when you begin to act as a representative of or consultant to any foreign entity, including a government, a government agency, a commercial business, or a person.

4. Security Violations/Vulnerabilities

You must report any known or suspected security violation or vulnerability of which you become aware, independent of who is responsible or at fault for the situation. Security violations/vulnerabilities include:

- the careless or unintentional failure to comply with security requirements for safeguarding classified information;
- the intentional disregard of security requirements;
- any failure to comply with security requirements, regardless of intent, that has resulted in the loss, compromise, or suspected compromise of classified information;
- the unauthorized receipt of classified material;
- significant vulnerabilities discovered in equipment or systems designed to protect classified information.

5. Espionage, Sabotage, Subversive Activities

You must immediately report any situation related to actual, probable, or possible espionage, sabotage, or subversive activities directed at the United States.

6. Suspicious Contacts

You must report:

- any efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise any cleared employee;
- any contact by a cleared employee with known or suspected intelligence officers from any country;
- any contact which suggests you or another employee may be the target of an attempted exploitation by the intelligence services of another country.

The Defense Hotline

The DoD maintains a hotline to provide an unconstrained avenue for employees to report, without fear of reprisal, known or suspected instances of serious security irregularities concerning government contracts, programs, or projects. Security recommends that the hotline number be used only when an employee feels that reporting a matter to MSU Office of Research/Facility Security Office would not be prudent. The Defense Hotline numbers are (800)424-9098 or (703)693-5080. In most instances, however, reports of suspected incidents of espionage, sabotage or serious security violations should be made to your local Security organization at the numbers listed above.