

The Concern. Failure to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate these operations.

Conditions that could raise a security concern and may be disqualifying include:

- (a) unauthorized entry into any information technology system;
- (b) unauthorized modification, destruction, manipulation or denial of access to, an information technology system or any data in such a system;
- (c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;
- (d) downloading, storing, transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system;
- (e) unauthorized use of any information technology system;
- (f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations or when otherwise not authorized;
- (g) negligence or lax practices in handling information technology that persists despite counseling by management; and
- (h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

Conditions that could mitigate security concerns include:

- (a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) the misuse was minor and done solely in the interest of organizational efficiency and effectiveness;

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification to appropriate personnel.

(d) the misuse was due to improper or inadequate training or unclear instructions.