

70 ISRW Critical Information List (CIL)

Current as of September 2011

Critical Information (CI) is defined as "specific facts about friendly intentions, capabilities, limitations, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment." The 70 ISRW CIL is a compilation of those areas identified in CIL of our subordinate groups (373 ISRG, 543 ISRG, 544 ISRG, 659 ISRG, 691 ISRG, 707 ISRG). A listing of general and specific 70 ISRW CI is as follows:

Operational:

1. Official information detailing the peacetime or wartime missions of the unit or subordinate or superior units, to include emergency or contingency plans.
2. Official information concerning coordination with or support to host base units or other outside agencies.
3. Association of nicknames or cover terms of classified or sensitive projects with the project, program or operation (i.e. special access programs/missions).
4. Increases or decreases in mission activity levels, to include critical manning issues.
5. Displaying knowledge of an adversary's capabilities.
6. The Wing or subordinate unit's success or weakness as identified in base or unit exercises, or actual operations and/or operational readiness status.
7. Planned or implemented organizational changes not yet released through Public Affairs channels, particularly any related to duty assignment changes.
8. Planned dates of mobility exercises, specific planned exercise scenarios.
9. Deployments, contingency or AEF tasking details.
10. Specific protective measures undertaken to protect mission, project or facilities.

Communications and Information:

1. Personnel data, Recall Roster
2. Unofficial discussion associating AFSCs, SEI, qualifications, etc., with specialty training, duty positions, areas of expertise and personnel strength compositions.
3. Critical communications frequencies, links, paths, OPSCOMM links or alternate paths.
4. Indications that certain information is classified.
5. Computer system configurations, capabilities, passwords, or security measures.
6. Information on itineraries of very important persons (general officers, civilian equivalent, or higher) or purpose of visit except as identified through Public Affairs channels.
7. Information about wing personnel, which could be used by hostile intelligence agencies for HUMINT targeting.
8. Performance Reports, Awards, Orders, or any other type of information distributed between NSA and Squadron Orderly Rooms

CONTINUED OTHER SIDE →

Logistics:

1. Official information regarding specific mission equipment installations and upgrades, to include personnel involved and dates.
2. Equipment/system capabilities and limitations, including logistics support or maintenance limiting factors or shortfalls.
3. Equipment Types and Capabilities (including all planned upgrades for existing equipment).
4. Host-tenant/inter-service support agreement for conduction of sensitive or classified operations.
5. Power or equipment outages impacting mission accomplishment.
6. Emergency destruction procedures, plans, and methods.

Administrative:

1. Information on TDY of our personnel to other units for contingency or non-contingency mission support, to include locations, timetables, and reasons for TDY.
2. Information or gossip on personnel issues, including the following: specialty codes, number of personnel assigned or departing, disciplinary actions, exploitable weaknesses (alcoholism, indebtedness, etc.), clearances, and positions trained on or being trained for.
3. Security procedures (to include physical, information, computer, and operations security).
4. Facility/compound security (strengths/weakness, alarms, layout, security violations, entry control procedures, system access controls).
5. Specific information concerning manpower levels, mission, or budget of units, deployed forces, or National Security Agency offices directed or supported by the 70 ISRW.
6. Degraded mission capabilities resulting from manpower, funds, equipment, or communications problems.
7. Information regarding security violations, on-going investigations, or the result of such investigations.

70ISRWVA 10-701, (Prescribed by AFI 10-701)
OPR: 70OSS/OST 5 June 2012
Certified by: 70ISRW/CV (Col Michael C. Harasimowicz)
RELEASABILITY: There are no releasability restrictions on this publication.