Critical Information List (CIL) - EXAMPLE

1. OPERATIONS

a. Official information detailing the mission of the Department/Organization/Agency and its assigned offices to include emergency or contingency plans.
b. Official information concerning coordination with or support to the Department/Organization/Agency or outside agencies.
c. Increases or decreases in mission activity levels to include critical manning issues.
d. Displaying knowledge of an adversary's capabilities
e. Planned or implemented organizational changes not yet released through Public Affairs, particularly any related to duty assignment changes.
f. Planned dates or other details of exercises and exercise scenarios.
g. Deployment timelines and schedules, contingency or Department/Organization/Agency tasking details.
h. Specific protective measures undertaken to protect mission, project, or facilities.
i. Details of security plans.

2. COMMUNICATIONS AND INFORMATION

a. Personal data
b. Recall rosters, personnel listings, e-mail listings, and office directories.
c. Continuity, backup and recovery plans.
d. Standard Operating Procedures, Concept of Operations and related publications.
e. Continuity of Operations (COOP) information to include: COOP procedures, dates, locations, and purpose of COOP exercises/scenarios, procedures for conducting vulnerability assessments.
f. Unofficial discussion associating Department/Organization/Agency's qualifications, with specialty training, duty positions, areas of expertise and personnel strength compositions.
g. Critical communications frequencies, links, or paths.
h. Employee's telework locations and schedules.
i. Indications that certain information is classified.
j. Computer system configurations, capabilities, efficiencies, passwords, or security measures.
k. Information on itineraries of very important persons or purpose of visit except as identified through Public Affairs.
l. Movements, locations, and daily calendar of senior leadership.
m. Information about Department/Organization/Agency personnel, which could be used by hostile intelligence agencies for Human Intelligence (HUMINT) targeting.
n. Systems availability and scheduled maintenance timelines.
o. Communications plans.

3. LOGISTICS/EQUIPMENT

a. Official information regarding specific mission equipment installations and upgrades, to include personnel involved dates.
b. Location of Department/Organization/Agency has deployed systems.
c. Equipment/System capabilities and limitations, including logistics support or maintenance irregular factors or shortfalls.
d. Equipment types and capabilities, to include all planned upgrades for existing equipment.
e. Network specifications and capabilities, network vulnerabilities and intrusion detection systems.
f. Support agreements for conducting sensitive or classified operations.
g. Power or equipment outages affecting mission accomplishment.
h. Emergency destruction procedures, plans and methods.

4. ADMINISTRATIVE

a. Official travel information of personnel, to include locations, timetables, and reasons for official travel.
b. Information on personnel issues, including the following: number or personnel assigned or departing, and disciplinary actions.
c. Security procedures to include physical, information, computer, and operations security.
d. Building/compound/facility/site security (strengths/weaknesses, alarms, layout, security violations, entry control procedures, system access controls).
e. Readiness response times, schedules, and other alert status information.
f. Specific information concerning staffing levels, mission, or budget of units, deployed teams, or offices directed or supported by Department/Organization/Agency.
g. Degraded mission capabilities resulting from staffing, funds, equipment, or communications problems.
h. Internal organizational charts or directories.
i. Information regarding security violations, on-going investigations, or the result of such investigations