INTELLIGENCE COMMUNITY DIRECTIVE 190

3 February 2015

Critical Information (CRITIC)

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order (EO) 12333, as amended; EO 13526; and other applicable provisions of law.

B. PURPOSE

1. This Intelligence Community Directive (ICD) establishes policy for the timely identification and transmission of critical information (CRITIC) pursuant to EO 12333, Section 1.3(b)(13).

2. This Directive rescinds Director of Central Intelligence Directive (DCID) 7/4, *Critical Information (CRITIC).*

C. APPLICABILITY: This Directive applies to the Intelligence Community (IC) as defined by the National Security Act of 1947, as amended; and to such elements of any other department or agency as may be designated an element of the IC by the President, or jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned.

D. POLICY

1. IC elements shall identify and report critical information consistent with this Directive and procedures provided by the Director, National Security Agency (DIRNSA). Critical information is information concerning possible threats to U.S. national security that are so significant that they require the immediate attention of the President and the National Security Council. Critical information includes the decisions, intentions, or actions of foreign governments, organizations, or individuals that could imminently and materially jeopardize vital U.S. policy, economic, information system, critical infrastructure, cyberspace, or military interests.

2. Critical information may originate with any U.S. government official in the IC. CRITIC reporting may be based on either classified or unclassified information. CRITIC reporting should be based solely on unclassified information only if that information is unlikely to be readily available to the President and the National Security Council.

3. An event that in isolation might not normally call for CRITIC handling may be evaluated by the reporting IC element as critical information if the event is closely linked to some other matter of considerable significance. Doubt about the CRITIC threshold, validity, or lack of confirmation should be resolved in favor of issuing a CRITIC.

4. Standard operating procedures for CRITIC handling are provided by the DIRNSA in the *Handbook of Standard Operating Procedures for Reporting Critical Information*, or U.S. Signals Intelligence Directive CR1501, *Handling of Critical Information*, or successor documents.

E. EXAMPLES OF CRITIC EVENTS: The following are examples of events that meet CRITIC reporting requirements as described in Section D.1:

1. Hostile Acts

a. An attack or major act of sabotage against the U.S. or against U.S. or allied forces, installations, or vital properties outside of a war zone.

b. Outbreak of war involving at least one country that is closely linked to vital U.S. interests.

c. Significant hostile actions against vital U.S. interests in international territories, international waters, or space.

d. Hostile use of weapons of mass destruction (chemical, biological, radiological, or nuclear).

e. A physical attack on critical infrastructure that is closely linked to vital U.S. interests.

f. A cyberspace attack or an operation that causes a cyber-effect against information systems of national security interest, including U.S. or allied government, military, or civilian infrastructure or information systems, if the attack or operation affects command and control, continuity of government, or the provision of essential services.

g. Malicious cyber activity that has significant consequences, adversely affects U.S. national interests, or triggers an emergency cyber action.

2. Terrorist Acts

a. A terrorist act targeting vital U.S. interests.

b. Assassination or kidnapping of U.S. officials or world leaders.

c. Hostage-taking or killing of U.S. nationals abroad for political purposes.

3. Political Disruption or Instability

a. Political or military upheavals in countries considered to be closely linked to U.S. vital interests.

b. Incidents that significantly heighten tensions along international borders.

c. The escalation of civil wars or previously localized disturbances as a result of the entrance of foreign military forces.

d. A cyberspace attack or an operation that causes a cyber-effect that triggers political disruption or instability outside of the United States or its close allies that directly affects vital U.S. interests.

4. An event, including a cyberspace attack or cyber-effect, that creates or contributes to an immediate major humanitarian, environmental, or economic crisis.

F. ROLES AND RESPONSIBILITIES

1. The DNI will advise the Secretary of Defense concerning the communications requirements of the IC for the transmission of critical foreign intelligence.

2. The DIRNSA shall provide standard operating procedures for CRITIC handling, consistent with this Directive, in the *Handbook of Standard Operating Procedures for Reporting Critical Information* or U.S. Signals Intelligence Directive CR1501, *Handling of Critical Information*, or successor documents.

3. Heads of IC elements shall ensure timely CRITIC reporting by their elements, consistent with this Directive and applicable procedures.

G. EFFECTIVE DATE: This Directive becomes effective on the date of signature.

James R. Clapper
Director of National Intelligence

3 Feb 2015
Date