Department of Defense
INSTRUCTION

NUMBER 3000.08
January 5, 2010
Incorporating Change 1, November 19, 2010

USD(AT&L)

SUBJECT: Balanced Survivability Assessments (BSAs)

References: See Enclosure 1

1. PURPOSE. This Instruction establishes policy, assigns responsibilities, and provides procedures for the DoD BSA program to support References (a) through (ag) in accordance with the authority in DoD Directive 5134.01 (Reference (ah)).

2. APPLICABILITY. This Instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. A comprehensive and effective BSA program shall focus on DoD mission essential functions (MEFs), primary mission essential functions (PMEFs), the national essential functions (NEFs) they support, and their supporting systems, networks, architectures, infrastructures, and assets to ensure the continued and enduring operation of DoD nuclear command and control functions and the assurance of global command, control, communications, computers, and intelligence (C4I) capabilities and critical national and defense resources. The BSA program shall use both Blue Team and Red Team methodologies to enhance their security, survivability, and continuity across a broad spectrum of threats and hazards.

b. Commanders and Defense Agency and DoD Field Activity Directors at all levels have the responsibility and authority to assure their missions, provide a secure environment for their personnel, and take appropriate measures to actively protect the key DoD resources that support

DoD MEFs, PMEFs, or the NEFs they support. Nothing in this Instruction shall detract from, or conflict with, the inherent and specified authorities and responsibilities of the DoD Components and commanders.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. INFORMATION REQUIREMENTS. The annual list of candidate mission critical functions, systems, architectures, infrastructure, or facilities required in Enclosure 2 is exempt from licensing in accordance with paragraph C4.4.2 of DoD 8910.1-M (Reference (ag)).

8. RELEASABILITY. RESTRICTED. This Instruction is approved for restricted release. ~~Authorized users may obtain copies on the SECRET Internet Protocol Router Network from the DoD Issuances Web Site at http://www.dtic.smil.mil/whs/directives~~ *It is available to users with Common Access Card authorization on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives*.

9. EFFECTIVE DATE. This Instruction is effective immediately.

Ashton B. Carter
Under Secretary of Defense for
Acquisition, Technology, and Logistics

Enclosures
1. References
2. Responsibilities
3. Procedures
Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5105.62, "Defense Threat Reduction Agency (DTRA)," November 28, 2005
(b) DoD Directive O-5100.30, "Department of Defense (DoD) Command and Control (C2)," January 5, 2006
(c) DoD Directive S-5100.44, "Defense and National Leadership Command Capability (DNLCC) (U)," July 9, 2008
(d) DoD Instruction 3150.09, "The Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy," September 17, 2008
(e) DoD Directive S-5210.81, "United States Nuclear Weapons Command and Control, Safety, and Security (U)," August 8, 2005
(f) Secretary of Defense Memorandum, "Designation of Responsibilities for Combating Weapons of Mass Destruction (WMD) to Commander, US Strategic Command (CDRUSSTRATCOM)," January 6, 2005
(g) National Security Presidential Directive-28 (NSPD-28), "United States Nuclear Weapons Command and Control, Safety, and Security," June 20, 2003
(h) DoD Directive 5400.07, "DoD Freedom of Information Act (FOIA) Program," January 2, 2008
(i) DoD Directive 5134.08, "Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs (ATSD(NCB))," January 14, 2009
(j) National Security Presidential Directive 17, "National Strategy to Combat Weapons of Mass Destruction," September 14, 2002
(k) DoD Instruction 3020.45, "Defense Critical Infrastructure Program (DCIP) Management," April 21, 2008
(l) Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," October 25, 2005
(m) Secretary of Defense, "Transformation Planning Guidance," April 2003
(n) DoD Directive 5205.07, "Special Access Program (SAP) Policy," January 5, 2006
(o) DoD Instruction 2000.18, "Department of Defense Installation Chemical, Biological, Radiological, Nuclear and High-Yield Explosive Emergency Response Guidelines," December 4, 2002
(p) DoD Directive 3150.8, "DoD Response to Radiological Accidents," June 13, 1996
(q) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," December 8, 2008
(r) DoD Directive 5530.3, "International Agreements," June 11, 1987
(s) DoD Instruction 8910.01, "Information Collection and Reporting," March 6, 2007
(t) DoD Directive 3020.26, "Department of Defense Continuity Programs," January 9, 2009
(u) DoD Directive 3020.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005
(v) Unified Facility Criteria 4-010-1, "Unified Facility Criteria (UFC), DoD Minimum Antiterrorism Standards for Buildings," October 8, 2003
(w) DoD Instruction 2000.16, "DoD Antiterrorism (AT) Standards," October 2, 2006
(x) DoD Directive 2000.12, "DoD Antiterrorism (AT) Program," August 18, 2003

(y) National Security Presidential Directive-51/Homeland Security Presidential Directive 20, "National Continuity Policy," May, 2007

(z) Federal Continuity Directive 1, "Federal Executive Branch National Continuity Program and Requirements," February 2008

(aa) Federal Continuity Directive 2, "Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process," February 2008

(ab) DoD Manual 3020.45, Volume 1, "Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP)," October 24, 2008

(ac) DoD Manual 3020.45, Volume 2, "Defense Critical Infrastructure Program (DCIP): DCIP Remediation Planning," October 28, 2008

(ad) DoD Instruction 6055.17, "DoD Installation Emergency Management (IEM) Program," January 13, 2009

(ae) Chairman of the Joint Chiefs of Staff Instruction 6510.01E, "Information Assurance (IA) and Computer Network Defense," August 15, 2007

(af) Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs Memorandum, "Defense Critical Infrastructure Program Assessment Standards and Benchmarks (Ver 1.1)," June 7, 2007[1]

(ag) DoD 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998

(ah) DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))," December 9, 2005

(ai) Under Secretary of Defense for Policy, "Defense Critical Infrastructure Program (DCIP) Security Classification Guide," May 2007[1]

(aj) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," as amended

(ak) Defense Threat Reduction Agency (DTRA), "BSA Security Classification Guide," August 18, 2008[2]

[1] Available from ASD(HD&ASA)

[2] Available from DTRA/OP-CSAB

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS (USD(AT&L)). The USD(AT&L) shall:

a. Serve as the OSD single point of contact for BSA-related matters, normally operating through the Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs and in consultation with the Director, Defense Threat Reduction Agency (DTRA).

b. Provide strategic guidance and policy direction for and monitor scheduling, planning, programming, budgeting, funding, and execution of the BSA program.

c. Monitor resource requirements resulting from BSA trends and lessons learned in coordination with the Chairman of the Joint Chiefs of Staff, the Under Secretary of Defense (Comptroller), and in consultation with the Director, DTRA.

d. Serve as the principal DoD representative for BSA matters with other Federal agencies and with State, local, and other non-DoD entities.

e. Maintain this Instruction to enhance the survivability and reduce the vulnerability of systems, networks, architectures, infrastructures, and assets that support DoD MEFs, PMEFs, or the NEFs they support to a broad range of threats and hazards.

2. DIRECTOR, DTRA. The Director, DTRA, under the authority, direction, and control of the USD(AT&L), through the Assistant to the Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs, shall:

a. Within assessment resources, prioritize (in coordination with the Chairman of the Joint Chiefs of Staff and appropriate OSD staff sections), schedule, and conduct BSAs of systems, networks, architectures, infrastructures, and assets that support DoD MEFs, PMEFs, or the NEFs they support, including those associated with critical command and control, nuclear command and control, nuclear weapons surety, and high containment biological select agents and toxins (BSAT) biosurety, against a broad spectrum of threat and hazard environments to enhance their survivability and operability. This shall include analyses to identify systemic vulnerabilities in strategic systems and/or architectures. These assessments shall be conducted on a Blue Team or Red Team basis and limited to a specific mission area tailored to customer requirements. BSA schedules shall be compiled from candidate BSA lists submitted in accordance with guidance in this Instruction. DTRA shall initiate the scheduling process annually by sending appropriate correspondence soliciting BSA scheduling inputs to responsible entities designated in this Instruction. Director, DTRA, will notify DoD elements involved in the BSA nomination process when BSAs that have been nominated cannot be met.

b. Develop and maintain plans to surge additional assessment capabilities to meet contingency support scenarios.

c. Conduct BSAs requested by non-DoD entities of U.S. and allied mission critical functions, systems, networks, architectures, assets, and infrastructures against a broad spectrum of threat and hazard environments to enhance their survivability and operability within assessment resource and DoD priority constraints.

d. Coordinate with the Joint Staff, Deputy Director for Operations, as the central schedule deconfliction activity for all Service and Combatant Command assessments, Joint Staff integrated vulnerability assessments, DCIP assessments, and BSAs.

e. Ensure all personnel performing BSAs are trained and qualified in these procedures and maintain proficiency and currency in their respective specialty disciplines.

f. Provide appropriate physical and information assurance (IA) protection measures to control BSA results and data, and grant access to BSA results and data only to organizations authorized by the requesting DoD Component except as provided elsewhere in this Instruction.

g. Develop a BSA lessons learned program. On an annual basis, provide a report on the BSA program, including important trends and observations from recent BSAs.

h. Maintain a capability to provide follow-up technical assistance to assessed organizations and provide other specialized assistance within BSA areas of expertise.

i. Implement appropriate legal, security, and safety controls for all phases of Blue Team and Red Team BSA operations.

j. Support broader assessments on the defense and national leadership command capability (DNLCC) systems as defined in Reference (c).

k. Ensure BSAs incorporate widely recognized standards and benchmarks, to include appropriate mission essential task lists, into their assessment methodology.

3. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) shall, as the DoD Continuity Coordinator and single point of contact to the Federal interagency for continuity matters, coordinate with the Under Secretary of Defense for Intelligence (USD(I)) and the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) to provide input to the USD(AT&L) on recommended BSA program changes.

4. USD(I). The USD(I) shall:

a. Annually consolidate and provide to the Director, DTRA, a list of candidate intelligence functions, systems, architectures, or facilities for Blue Team and/or Red Team BSAs.

b. Upon request, provide inputs to USD(P) on recommended BSA program changes.

5. DIRECTOR, NATIONAL SECURITY AGENCY (NSA)/CHIEF, CENTRAL SECURITY SERVICE (CSS). The Director, NSA/Chief, CSS, under the authority, direction, and control of the USD(I), shall coordinate requirements for computer operations and communications specific support and other specialized expertise to support Red Team BSA efforts with the Director, DTRA. The level of support will be mutually agreed upon and provided as available.

6. DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY (NGA). The Director, NGA, under the authority, direction, and control of the USD(I), shall coordinate requirements for products and analysis to support the Red Team BSA efforts with the Director, DTRA. The level of support will be mutually agreed upon and provided as available.

7. ASD(NII)/DoD CIO. The ASD(NII)/DoD CIO shall:

a. Annually consolidate and provide to the Director, DTRA, a list of candidate network, network-centric, command and control, communications, non-intelligence space, information, and DNLCC systems, architectures, or facilities for Blue Team and/or Red Team BSAs.

b. Upon request, provide inputs to USD(P) on recommended BSA program changes.

8. ASD(HD&ASA). The ASD(HD&ASA), under the authority, direction, and control of the USD(P), shall:

a. Annually consolidate and provide to the Director, DTRA, a list of candidate defense critical infrastructure functions, systems, architectures, or facilities for Blue Team and/or Red Team BSAs. These defense critical infrastructures will focus on defense critical assets (DCAs) or Tier 1 task critical assets (TCAs) as determined by the critical asset identification process (CAIP) in support of the Defense Critical Infrastructure Program (DCIP).

b. Upon request, provide inputs to USD(P) on recommended BSA program changes.

9. HEADS OF THE DoD AND OSD COMPONENTS. The Heads of the DoD Components and OSD Component Heads other than USD(I), ASD(NII)/DoD CIO, and ASD(HD&ASA), shall:

a. Annually provide to the Chairman of the Joint Chiefs of Staff a list of candidate systems, networks, architectures, infrastructures, and assets that support DoD MEFs, PMEFs, or the NEFs they support for Blue Team or Red Team BSAs.

b. Annually, as part of the DoD PPBE cycle, determine the merit of subordinate BSA vulnerability mitigation resource requirement submissions for BSAs other than those on DCAs or TCAs; review the adequacy of resources proposed by them to determine whether they meet survivability and continuity objectives; and make recommendations to the Chairman of the Joint Chiefs of Staff on unresolved survivability and continuity requirements during programming and budget reviews. The management of vulnerability mitigation resource requirements from BSAs of DCAs or Tier 1 TCAs shall be done in accordance with Reference (k).

10. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Chairman of the Joint Chiefs of Staff shall:

a. Serve as the principal military advisor to the Secretary of Defense for all DoD BSA issues.

b. Advise the Secretary of Defense of any changes needed to meet BSA program objectives.

c. Annually solicit Combatant Commands and Military Department Blue Team and Red Team BSA requirements and provide a consolidated list to the Director, DTRA.

d. Annually, as part of the DoD Planning, Programming, Budgeting, and Execution (PPBE) process, assist the DoD Components in determining the merit of BSA vulnerability mitigation resource requirement submissions for BSAs other than those on DCAs or TCAs, review the adequacy of resources proposed by the Military Departments to determine whether they meet survivability and continuity objectives and support combatant commanders' programs, and coordinate and make recommendations on unresolved survivability and continuity requirements during programming and budget reviews.

11. COMMANDER, U.S. SPECIAL OPERATIONS COMMAND (CDRUSSOCOM). The CDRUSSOCOM shall coordinate requirements for special operations assets needed to support Red Team BSA efforts with the Director, DTRA. The level of support will be mutually agreed upon and provided as available.

12. COMMANDERS OR DIRECTORS OF ENTITIES SUBJECT TO BSAs. Commanders or directors of entities subject to BSAs shall:

a. Ensure BSA recommendations are evaluated via internal risk assessment and risk management programs and implemented as appropriate to acceptable risk. To facilitate situational awareness, ensure information on significant accepted or residual risks is available to higher headquarters or cognizant officials responsible for complementary programs, if applicable to assessed mission areas.

b. Identify to the appropriate DoD Component any additional resource requirements to implement mission critical protection and survivability measures. For emergent and/or emergency requirements that cannot be met through other means, submit resource requirements through the appropriate DoD Component to the Chairman of the Joint Chiefs of Staff for consideration.

c. Commanders or directors responsible for systems, networks, architectures, infrastructures, and assets that support critical command and control, nuclear command and control, nuclear weapons surety, and high containment BSAT biosurety, per References (a) through (g), shall have them undergo BSAs, and shall consider requesting a follow-on Blue Team BSA after a period of 5 years has passed or after major configuration or mission changes.

d. Commanders or directors responsible for systems, networks, architectures, infrastructures, and assets that support DoD MEFs, PMEFs, or the NEFs they support should have them undergo BSAs, and should consider requesting a follow-on Blue Team BSA after a period of 5 years has passed or within 1 year after major configuration or mission changes. Defense critical infrastructure BSAs will focus on DCAs or Tier 1 TCAs in support of the DCIP.

e. Owners of planned major new systems, networks, architectures, infrastructures, and assets that support DoD MEFs, PMEFs, or the NEFs they support should consider requesting a BSA or a BSA technical review of plans during the planning or requirements phase to ensure security and survivability measures are appropriately incorporated.

ENCLOSURE 3

PROCEDURES

1. DOD BSA PROGRAM

a. The mission of DTRA is to safeguard the United States and its allies from weapons of mass destruction (WMD) (e.g., chemical, radiological, nuclear, and high-yield explosives) by providing capabilities to reduce, eliminate, and counter the threat and mitigate its effects. The BSA program is organized under the DTRA Combat Support Assessments Division.

b. BSAs are defined in the Glossary. BSA recommendations focus on operational processes and procedures, improved planning and analysis, low-cost procurement, and longer-term design changes.

c. BSAs are tailored to meet the needs of the customer, focus on continuity of specific mission areas, and revolve around measures that can be taken to improve mission assurance and survivability against an "all threats and hazards" approach (e.g., natural disasters, accidents or incidents, disruptive actions, hostile forces, malicious insiders, and WMD attack effects). Thus, Blue Team BSAs are not geographically oriented (e.g., an entire military base with multiple tenants or missions); however, Red Team BSAs may have a geographical orientation. BSAs provide multidisciplinary integration, broad applicability, and security and survivability support for systems, networks, architectures, infrastructures, and assets that support DoD MEFs, PMEFs, or the NEFs they support to ensure the continued and enduring operation of our nuclear command and control functions, and the assurance of global C4I and other critical national and defense capabilities and resources.

d. BSAs shall be a tool in DoD Components' integrated risk management plans and processes. Mission-focused, multidisciplinary BSAs complement other joint, Service, or Combatant Command assessments that may be focused on a single discipline or area such as antiterrorism and force protection (AT/FP) or IA.

e. DTRA's role in DoD integrated vulnerability assessments (IVA) includes the use of BSAs in support of mission assurance system and architecture characterizations at the strategic national level. BSAs should also be called upon to assist Combatant Commands in mission decomposition. In this role, BSAs should be considered for an integrated assessment approach to systems, networks, architectures, infrastructures, and assets that are deemed DCAs or Tier I TCAs. The BSAs use an "all threats and hazards" approach to debilitating events and a team of diverse subject matter specialists to support the Department of Defense in assessing defense critical infrastructures as part of Reference (k). The approved way-ahead for DoD vulnerability assessments concluded that addition of the BSA capability to the IVA and an associated mission decomposition process is essential, in conjunction with modified Joint Staff integrated vulnerability assessments and a self-assessment capability, to meet the assessment requirements of the Department's critical infrastructures and assets. These changes form the basis of the new DoD assessment program to better serve commanders in the field while allowing responsible

DoD entities to execute their mission assurance responsibilities as outlined in current policy issuances.

f. An infrastructure's criticality, as determined through the DoD mission-based CAIP (see Reference (ab)), vetted against likely threats and hazards as determined through an enhanced threat and hazard assessment should determine where BSAs are best employed for DCIP assessments. To facilitate DCIP mission assurance assessments, current DCIP assessment benchmarks and standards (ASD(HD&ASA) Memorandum (Reference (af))), shall guide the BSA team. The Defense Critical Infrastructure Program (DCIP) Security Classification Guide (Reference (ai)) guides the marking, processing and handling of related DCIP information. The resulting assessment report shall be focused to provide installation commanders and/or asset owners the necessary inputs for preparing appropriate risk decision packages to meet the requirements of Reference (k).

g. Systems, networks, architectures, infrastructures, and assets that support critical command and control, nuclear command and control, nuclear weapons surety, and high-containment BSAT biosurety, per References (a) through (g), shall undergo BSAs. Responsible commanders or directors shall consider requesting a follow-on Blue Team BSA after a period of 5 years has passed or after major configuration or mission changes.

h. Systems, networks, architectures, infrastructures, and assets that support DoD MEFs, PMEFs, or the NEFs they support will undergo periodic BSAs, when requested by responsible commanders or directors. BSAs on those defense critical infrastructure assets identified as DCAs or Tier 1 TCAs may occur at least every 5 years or within 1 year of major configuration or mission changes.

i. BSAs nominally consist of three phases: pre-assessment, assessment, and post-assessment. The timelines and specific activities in each of these phases vary between Blue Team and Red Team BSAs. Sections 2 and 3 of this enclosure provide details about these differences.

j. Upon request, DTRA provides its customers post-BSA continuing technical support, that is, a capability to "reach back" and access its subject matter specialists to address follow-on issues that may arise.

k. DTRA, not less than annually, evaluates Blue Team and Red Team BSA results to identify trends and lessons learned, such as systemic, cross-organization, or enterprise-wide vulnerabilities that affect multiple systems, organizations, or programs. DTRA provides recommendations to address these issues to the cognizant authorities (e.g., Joint Staff, ASD(HD&ASA), ASD(NII/DoD CIO), USD(I), USD(AT&L)) for consideration or action, as appropriate.

l. (FOUO) Due to the extensive damage that can be done to critical U.S. capabilities or missions if unauthorized access to and subsequent exploitation of BSA results occurs, the distribution of individual BSA results is controlled. They are provided only to the assessed organization; the Joint Staff and their Combatant Commander and Military Service, as applicable; the organization that requested or directed the BSA; and organizations required by Reference (ae). For designated DCAs or TCAs, BSA reports will also be distributed in accordance with the requirements of Reference (k). DTRA does not distribute specific BSA results elsewhere without the express permission of the assessed organization or the BSA sponsor, as applicable. The customer's or the applicable program security classification guidance (e.g., DCIP) or, lacking these, the BSA Security Classification Guide (Reference (ak)) determines the security classification of BSA results. If multiple security classification guides apply to a BSA, the BSA team will apply the most stringent requirements. If appropriate, for extremely sensitive missions, BSA results and materials do not leave the customer's control.

m. (FOUO) BSA vulnerability and mission impact data as well as information on actual mitigation measures shall be physically and electronically protected in accordance with national and DoD classified and sensitive information laws, policies, and operations security requirements. Authorization to release BSA reports and findings resides with the assessed organization; the Joint Staff and their combatant commander and Military Service, as applicable; or the organization that requested or directed the BSA. Non-attribution highlights of BSA assessments may be used by DTRA in briefings or reports to higher-level organizations in the Department of Defense.

2. DTRA BLUE TEAM TECHNICAL SUPPORT

a. Requests for DTRA Blue Team technical specialist support outside of formal BSAs shall be accommodated as resources permit. Outside requests for assistance must be consistent with the DTRA Blue Team mission. These requests may include participation in working groups, special studies, technical and analytical support, survivability reviews of planned facilities, and small focused assessments.

b. Requests for DTRA Blue Team technical specialist assistance should be submitted to DTRA.

3. DTRA BLUE TEAM BSA METHODOLOGY

a. The Blue Team BSA program provides a tool to help protect critical national, DoD, and other Government agency missions, functions, assets, infrastructures, and their continuity from threats ranging from malevolent acts by malicious insiders or adversaries (e.g., nuclear weapons, other WMD, terrorist attacks, and sabotage) to accidents and acts of nature. These assessments are done in full and open cooperation with the host organization, providing an "inside looking out" perspective. Blue Team BSAs are accomplished with a Government-led contractor team of specialists.

b. (FOUO) During the pre-assessment phase, DTRA conducts a site visit, normally a month or more prior to the onsite assessment phase, to inform the local commander and staff on the BSA process; provide them an overview of BSA data requirements; finalize the scope of and timeline for the BSA; obtain and review specifics on the mission and critical information, systems, or elements, to include the baseline elements of information when assessing a DCA or TCA; coordinate the use of IA tools on the customer's networks; and address administrative support issues. The level of support will be mutually agreed upon during this phase. BSA subject matter specialists conduct open-source research to prepare for the assessment during this phase. When assessing a designated DCA or TCA, DTRA shall coordinate with the appropriate defense infrastructure sector lead agent (DISLA), as designated in Reference (u), and it will compare received mission information, system, and element data to the CAIP data.

c. (FOUO) During the onsite assessment phase of the Blue Team BSA, team members identify and assess the assets, information, and telecommunications networks, systems, equipment, sites, and people critical to accomplishing a specific mission area. They then identify mission vulnerabilities, assess mission impact if the vulnerabilities are successfully exploited, and develop recommendations to mitigate or eliminate them. Emphasis is on identifying single point vulnerabilities (see Glossary). The assessed organization is provided an outbrief of significant findings and recommendations before the team departs the site.

d. During the post-assessment phase, analysis of findings is completed and a detailed written report is prepared and forwarded to the assessed organization within 60 days of completion of the onsite portion of the BSA. DTRA provides follow-on support, when requested, to assist in the implementation of recommendations or in the technical review of design and development of new architectures, equipment, processes, or procedures.

e. (FOUO) The BSA process accounts for changes in mission criticality over time or operational phases, required reconstitution times, and the availability, readiness, and endurance of alternate facilities, among other factors and when applicable. BSA team members follow formal standard operating procedures, one for each technical discipline, focused on mission survivability against the widest spectrum of threats or hazards. The integrated team methodology and discipline-specific guidelines ensure that all relevant topics and cross-disciplinary interdependencies are examined. The BSA process is based upon and captures the insights, best practices, and expertise of Government and industry as well as DoD, joint, and other U.S. Government doctrine and policy. This process is implemented based upon the sound judgment and experience of the BSA team members.

f. (FOUO) BSAs use mission survivability impact as the criteria to assess the criticality of each identified vulnerability. That is, if an identified vulnerability is exploited by whatever means, what will be the operational impact on the assessed entity's ability to execute the assessed mission areas? To aid in the discovery of vulnerabilities, BSA teams use tools such as survivability, security, or surety benchmarks and standards or mission performance, reliability, or policy requirements, as relevant to the mission areas being assessed and as applied using the context of mission survivability. Examples of standards and benchmarks used include those for BSAT biosurety, nuclear surety, DCIP, unified facilities criteria, and the AT/FP program. Examples of performance, reliability, or policy requirements include those for nuclear command and control processes, continuity of operations, IA, and MEFs and task lists. When executing Blue Team BSAs on DCIP assets, BSA teams will use approved DCIP standards and benchmarks as a tool to ensure a consistent focus on defense critical infrastructures.

g. (FOUO) Blue Team BSA core competencies include structural protection and response (to include blast effects modeling and consideration of AT/FP standards), information operations (e.g., computer networks, IA tools use, operations security), telecommunications (e.g., video, voice and data, commercial and military), utility subsystems (e.g., power and heating, ventilation, and air conditioning reliability and endurance), emergency operations (e.g., emergency preparedness, fire protection, emergency response, disaster control and recovery, continuity of operations), electromagnetic protection (e.g., electromagnetic pulse and radio frequency weapon susceptibility, lightning protection), physical security, surveillance operations, and WMD protection. All team members are formally trained and qualified. Additional specialist disciplines (e.g., medical, explosive ordnance disposal) are added to Blue Team BSAs as required to meet specific assessment needs.

h. Nominally, a Blue Team BSA team consists of a Government lead, a mix of 10 to 15 contractors in the technical disciplines, as described in paragraph 3g. of this enclosure, and requisite administrative support. Since the team is tailored to meet the requirements of the customer, additional personnel are added as necessary, based on the size and complexity of the assessment.

i. The onsite portion of a Blue Team BSA is generally 2 weeks. Blue Team BSAs are tailored to the customer; hence, this onsite phase could be of shorter or longer duration, dependent on the size, scope, and complexity of the assessment.

4. DTRA RED TEAM BSA METHODOLOGY

a. (FOUO) The Red Team BSA program is a DoD effort that emulates threats ranging from a foreign intelligence service to a well-funded terrorist group or a capabilities-based threat. While the senior leadership and limited, designated trusted agents in the assessed organization are aware of these assessments, the majority of the assessed organization’s personnel are not made aware of the assessment. Red Team BSAs provide an “outside looking in” perspective. Red Team members are provided no insider knowledge of the elements of the architecture, organization, or system being assessed. Nominally, a Red Team BSA team consists of a Government lead, a mix of DTRA contractors, requisite administrative support, and tailored augmentation from DTRA’s Red Team DoD partners.

b. (FOUO) A DTRA Red Team BSA effort is typically a system-wide or architecture-wide vulnerability assessment of an organization. Each Red Team BSA is requested by a DoD Component or other Government activity. The Secretary of Defense or Deputy Secretary of Defense approves Red Team BSAs of missions or organizations external to the Department of Defense, while the Director, DTRA, approves those internal to the Department of Defense. These efforts can last from several weeks to many months. Knowledge of these efforts is strictly limited to senior leadership, trusted agents, and white cell controllers within assessed entities.

c. (FOUO) During the pre-assessment phase, DTRA educates the customer on the Red Team BSA process and develops assessment objectives, ground rules, and timelines. DTRA conducts final coordination with its partners for requisite team augmentation or support and establishes appropriate safety and security controls and procedures. DTRA obtains legal approvals from appropriate authorities and develops detailed ground rules to ensure that real-world integrity of assessed operational systems and safety of all personnel is not compromised.

d. (FOUO) During the assessment phase, team members identify and assess organization components and assets, identify mission vulnerabilities, and exploit them in accordance with the pre-approved ground rules and legal reviews. The team conducts collection efforts to emulate hostile intelligence operations. The resulting information is integrated to provide target assessments and to revise collection requirements. The team then evaluates and validates, through demonstration, physical and electronic vulnerabilities identified during the targeting process.

e. During the post-assessment phase, analyses are completed and a detailed briefing and written report are provided to the assessment requestor within approximately 60 days after completion of the assessment phase of the BSA. DTRA provides follow-on continuing support, when requested, to assist in the implementation of recommendations or in the technical review of design and development of new architectures, equipment, processes, or procedures.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(HD&ASA)	Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
ASD(NII/DoD CIO)	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
BSA	balanced survivability assessment
BSAT	biological select agents and toxins
C4I	command, control, communications, computers, and intelligence
CAIP	critical asset identification process
CDRUSSOCOM	Commander, U.S. Special Operations Command
DCA	defense critical asset
DCIP	Defense Critical Infrastructure Program
DNLCC	defense and national leadership command capability
DISLA	defense infrastructure sector lead agent
DTRA	Defense Threat Reduction Agency
IA	information assurance
IVA	integrated vulnerability assessment
MEF	mission essential function
NEF	national essential function
NGA	National Geospatial-Intelligence Agency
NSA	National Security Agency
PMEF	primary mission essential function
PPBE	Planning, Programming, Budgeting, and Execution
PSA	Principal Staff Assistant
TCA	task critical asset
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
WMD	weapons of mass destruction

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

BSA. Multidisciplinary, integrated, performance-based, mission survivability assessments to identify and quantify vulnerabilities in systems, networks, architectures, infrastructures, and assets that support DoD MEFs, PMEFs, or the NEFs they support, to assess the mission impact if the vulnerabilities were successfully exploited, and to recommend measures to remediate or mitigate the vulnerabilities.

critical infrastructure protection. Defined in Joint Publication 1-02 (Reference (aj)).

criticality assessment. Defined in Reference (aj).

DCA. Defined in Reference (u).

defense critical infrastructure. Defined in Reference (u).

dependency. Defined in Reference (u).

design basis threat. Defined in Reference (v).

infrastructure. The framework of networked assets that comprise identifiable industries, institutions, or distribution capabilities that enable a continued flow of goods and services.

level of protection. Defined in Reference (v).

mission assurance. Defined in Reference (u).

MEF. Defined in Reference (t).

mitigation. Defined in Reference (u).

physical security. Defined in Reference (aj).

reconstitution. Defined in Reference (k).

remediation. Defined in Reference (u).

risk. Defined in Reference (u).

risk assessment. Defined in Reference (u).

risk management. Defined in Reference (c).

security. Defined in Reference (aj).

security engineering. Defined in Reference (v).

single point vulnerability. Selected equipment, processes, procedures, infrastructures, and/or key positions (or a multiple or combination that is collocated) that, if destroyed or denied, would result in the loss or severe degradation of mission.

TCA. Defined in Reference (k).

vulnerability. Defined in Reference (aj).