MILITARY SPECIFICATIONS AND STANDARDS REFORM PROGRAM (MSSRP)

CRITICAL PROCESS ASSESSMENT TOOL (CPAT)

<u>SURVIVABILITY</u>

14 August 1998

SMC/AXMP

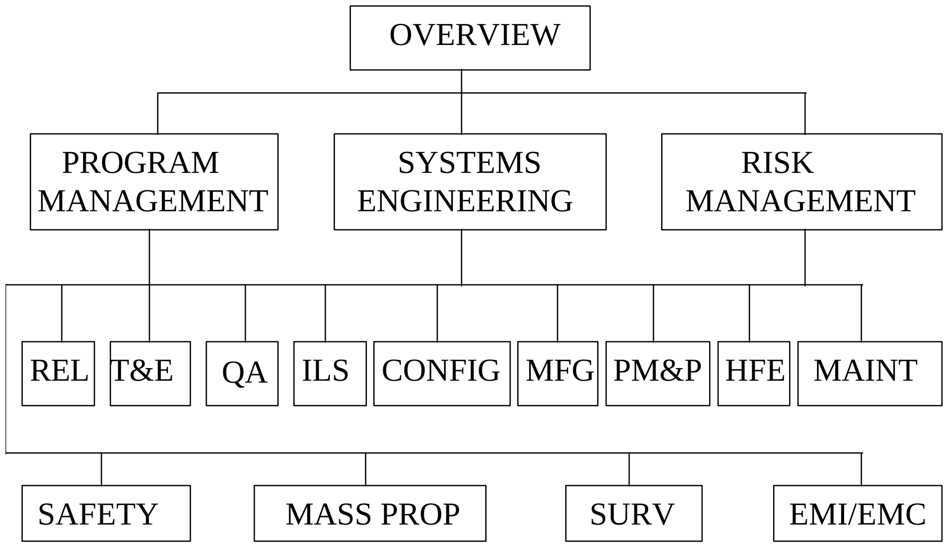
Critical Process Assessment Tool (CPAT)

Survivability

Table of Contents

FOREWORD

This Critical Process Assessment Tool (CPAT) is intended for use during the development of a solicitation and during the management of the acquisition through the end of the program. As a guide, it specifically addresses the Survivability critical process, but should be used in conjunction with other CPATs which address other functional areas when working in an Integrated Product Team (IPT) environment. Just as the survivability function must interact with other disciplines within the IPT, this CPAT fits within a framework of other CPATs. The figure below provides a depiction of the interrelationship of the CPAT structure.



The Overview CPAT provides a description of the tool's format, guidance on its usage, and a overview of the acquisition process, so it should be consulted by the first time reader. The Program Management, Systems Engineering, and Risk Management CPATs are the overarching CPATs for the IPT process and contain specific acquisition process information, integrating the processes of the other CPATs. In order to reduce redundancy, the reader will find that they are referenced throughout the other CPATs.

The remaining CPATs address specific functions that input to the IPT process. While the focus is on individual functions, many interface with one another and therefore contain references to each other.

The Critical Process Assessment Tools (CPATs) are intended as aids for project officers and project engineers in preparing (1) Requests for Proposals (RFPs), (2) developing source selection standards, (3) performing technical evaluations and fact-finding, and (4) participating in or reviewing contract execution after contract award. The CPATs are applicable to processes that, because of risk, are critical to contract execution. Survivability is a critical process for system and item development, modification, or even off-the-shelf acquisition since survivability requirements directly impact the military utility of a system, the cost, and the technical risk in design development, design verification, production and lifecycle maintenance.

1.0 Introduction to the Survivability CPAT

1.1 Description of the Survivability Critical Process

Survivability as defined in DoD 5000.2-R (March 15, 1996) is the capability of a system and crew to avoid or withstand a manmade hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission. In practice, however, this definition of survivability is often expanded beyond manmade hostile environments to include the severe effects of certain natural environments. This CPAT describes a process for implementing the survivability function into the systems acquisition process and evaluating its adequacy and performance. The process described in this CPAT by which the survivability function can be accomplished is composed of three main activities: Survivability Management, Survivability Engineering, and Survivability Operations. Survivability Management provides the structure for organizing, planning, control, and risk management. Survivability Engineering is composed of requirements development, survivability analysis, information management, and monitoring. Survivability Operations consists of survivability design, test, failure reporting, and corrective actions.

A satellite system is typically composed of a space segment (constellation of satellites), a user segment (ground-based, air-based, and/or sea-based terminals), and a control segment (usually a ground based facility or facilities) which provides the command link controlling of space assets and allocation of satellite resources to users. For the space segment, survivability must address the harsh natural space environment as well as man-made hostile threats. These natural environments include phenomena such as the following: ionizing radiation due to charged particles trapped in the earth's magnetosphere, solar flare protons and electrons, cosmic ray heavy ions; and micrometeorites. The natural radiation environment can degrade satellite materials and affect electronics performance. Solar flares and cosmic rays can induce what are known as Single Event Upsets (SEUs) in sensitive electronics of space-based equipment as well as potentially cause performance problems in ground-based equipment. Micrometeorites can damage satellite structure and components.

Man-made hostile environments and threats either current or projected over the operational life of a system which can jeopardize space segment survivability may include phenomena such as the following: attacks by ground or airborne directed energy weapons (lasers, RF and microwaves, neutral particle beams, or plasma beams), orbiting debris including that due to antisatellite testing, space explosions or collisions (space mines), exoatmospheric nuclear bursts, and the effects of direct, near neighbor, or distant attacks by Anti-satellite (ASAT) weapons (conventional, nuclear, or directed energy). Depending on the basing of the user and control segments, there may be requirements for these terminals or platforms to survive the effects of various conventional weapons (e.g., blast, shock, debris), nuclear weapons (e.g., blast, shock, radiation, thermal, electromagnetic pulse), directed energy weapons, as well as chemical or biological weapons attacks. For some systems, the threat of system sabotage against the user and/or control segments through physical attack or computer system penetration are system security issues which impact the survivability of a system. Information warfare may be considered a special variant of a sabotage threat.

System survivability must consider threats directed specifically at the communications and data links or associated hostile environments which degrade performance of these links between the various system segments. Electronic warfare jamming threats can be directed at the uplink (i.e., at the satellite), downlink (i.e., user and control segments), or even in some cases directed at the satellite-to-satellite crosslinks. RF interceptor threats may be identified which drive Low Probability of Intercept (LPI) requirements to insure communications and operational security as well as system surivivability. Natural ionospheric and nuclear burst induced scintillation cause random fluctuations in propagated signals which can degrade system link performance. Furthermore, signals can be absorbed as they pass through ionized regions, and, in some, cases total communications or data link blackout may occur.

The survivability process involves not only working with the intelligence community (the service's intelligence agency and the Defense Intelligence Agency) to identify threats and threat scenarios a system must be designed to withstand either near term or over the projected life of a system, but also with the operational community to define what a reasonable expected performance of the system should be against these threats to meet operational mission needs. Note that the DoD 5000.2 definition of survivability states that survivability is "the capability of a system and crew to avoid or withstand a manmade hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission." In other words, depending on the mission, certain temporary outages of a system may be acceptable under certain scenarios or there may be allowable degradations of performance after exposure to certain hostile environments. In effect, survivability is not a process for insuring the physical survivability of a system but rather survivability is a process for insuring the functional and performance survivability of a system. It is system's required functional and performance survivability against a threat environment which drives survivability design.

The survivability function is part of the system engineering process. The survivability function translates the natural environment and threats into detailed environments, defines system survivability design and verification requirements against these environments, and allocates design performance and verification requirements throughout the system down to the piecepart level and across all interfaces. The survivability function develops design guidelines and databases to support design development, oversees requirements verification, and assures survivability is jeopardized during the production process. The survivability process must also identify what is necessary to maintain system survivability throughout the life of the system. This may include special satellite storage and test requirements, and periodic hardness surveillance and maintenance activities for non space-based system assets.

1.1.1 Summary of the Survivability Process During Each Phase

The Survivability process plays an important role during each phase of acquisition. During Concept Exploration (Phase 0), the primary focus for survivability working in support of the systems engineering process is what level of survivability and general approaches for attaining that level of survivability provide the military capability defined by the Mission Need Statement (MNS). Factors that must be considered include the intended use of the system, interfaces with other systems, the levels of conflict and associated potential scenarios, projected threats over the lifetime of the system (including possible reactive threats to the fielding of this system), technical risk, and cost.. This is the time when mission area analyses are initially performed to identify capabilities required to meet the military needs as defined in the MNS. Survivability unquestionably becomes a key factor in evaluating military utility. Survivability efforts require close coordination both with the user community to understand how the system is expected to be used and with the intelligence community regarding current and projected threats. All threats used to design or assess system performance must be based on Defense Intelligence Agency (DIA) validated documents. During Concept Exploration, several contractors may be tasked to address high level system architectural issues associated with a variety of concepts or approaches which can impact the level of survivability ultimately achieved or directly reflect alternatives to counter specific threats. These system issues include such architectural issues as the number of satellites in the constellation, the orbit altitude and general orbital characteristics, satellite weight and power, degree of satellite autonomy (i.e., the capability of the space segment to perform without ground intervention), communications link architectures and options, as well as general survivability approaches such as whether a satellite will be capable of evasive or avoidance maneuvering against directed threats as well as whether possible countermeasures (such as decoys and antisimulation devices) will be employed against certain types of threats. Each of these system attributes profoundly affects both survivability and system cost. The Operational Requirements Document (ORD) prepared by the user or user's representative is a key vehicle for documenting the results of mission area analyses, the associated minimum acceptable performance required by the system (threshold values), and the desired capabilities (objective values). A government agency is also tasked to prepare the initial Cost and Effectiveness Analysis (COEA) during Phase 0 to support a Milestone I decision. The COEA provides an independent evaluation of the costs, benefits, military utility, and effectiveness of alternative approaches and concepts.

In the Program Definition and Risk Reduction phase (Phase I) it is important for contractors and the government to identify any new or critical technologies, components, or subsystems whose function is related to survivability and to devise a means for demonstrating/validating that the function will be performed properly. Technologies to meet threshold and objective survivability requirements defined in the ORD will be studied, alternatives identified, military utility further analyzed, and costs refined. The ORD will be refined by the user and cost/risk/utility tradeoffs documented in contractor/government analyses and an updated COEA will support decisions regarding the top level system requirements.

During Engineering and Manufacturing Development (EMD) (Phase 2) the primary focus of survivability is to perform or assist in cost/schedule/risk trade studies that impact survivability performance, determine requirements allocations and insure the proper flowdown of survivability design and verification requirements (i.e., the flowdown of requirements from the system to the segments and their interfaces, to the hardware and software configuration items and their interfaces, all the way down to the piecepart level), provide survivability design guidelines and databases for product engineering, audit survivability design implementation, and oversee and assess all survivability design verification activities. EMD is also the period when hardness assurance tests and controls which must be implemented during production are defined, acceptance tests are specified as needed, special satellite storage and test requirements are identified, and hardness maintenance/surveillance plans are established for primarily the non-spaceborne assets over the system life.

Prior to proceeding into full-rate production or deployment, Operational Test and Evaluation (OT&E) activities performed by and independent agency must address the survivability performance of the system. Evaluations are typically based on some combination of test and analysis. Furthermore, Live Fire Test and Evaluation (LFT&E) is required by law on any covered system, major munition program, missile program, or product improvement to a covered system, major munition program, or missile program before it can proceed beyond low-rate initial production. Per DoD 5000.2, a covered system is any vehicle, weapon platform, or conventional weapon system that includes features designed to provide some degree of protection to users in combat and that is an ACAT 1 or II program. Furthermore, LFT&E survivability testing is stipulated to begin at the component, subsystem, and subassembly level, culminating with tests of the complete covered system or program, or covered product improvement configured for combat.

During Production, Fielding/Deployment, and Operational Support (Phase 3), the survivability function oversees all survivability acceptance testing [e.g., a) piecepart radiation hardness assurance testing consisting of lot acceptance and screening tests, b) end item acceptance tests], and assesses survivability impacts due to any component changes caused by part or material nonavailability, part obsolescence, or manufacturing process improvements. Survivability evaluates the results of periodic hardness surveillance tests of the operational system, and insures the hardness maintenance program is being executed properly.

During Demilitarization and/or Disposal, survivability may be required to support specialized tasks depending on the specific design of the system or designated modified uses of the system as new or replacement systems are fielded.

1.1.2 Contribution to Mission Success

Survivability forms a cornerstone for any military system to successfully meet its peacetime and wartime missions. Survivability can pose unique challenges for a military acquisition for which there may be no civilian or commercial counterpart. Failure to adequately perform the survivability function can ultimately mean mission failure. In the best of unpleasant outcomes resulting from failure to adequately perform the survivability function, problems are discovered late in the design or verification process. Modifications at this point in time can cause severe cost and schedule impacts to the program. In the worst of scenarios, problems are never surfaced because of inadequate survivability design, verification, surveillance, or maintenance programs prior to system employment in a hostile engagement. Unanticipated system performance degradation or destruction against the hostile threat will lead to mission failure and potentially endangerthe success of the military engagement.

All satellite programs will have some survivability requirements if only to operate within the harsh natural space environment. The vacuum of space induces spacecraft material outgassing which can degrade optical sensors and thermal control materials. The natural space radiation and micrometeorite environment also cause degradation and damage. Solar Flares and Cosmic Rays cause single event upsets (SEUs) in modern micron-scale electronic circuits and can impact performance of spaceborne and ground assets.

Man-made hostile threats depend on the level of conflict for which a system is intended to operate, as well as reactive threats (i.e., threats designed specifically against the system) which may evolve depending on the enemies' perceived significance of the system's mission or perceived vulnerabilities. Man-made hostile threats can range from information warfare (e.g. Trojan horse software penetrations) to electronic warfare (jamming, spoofing) to collateral damage caused by attacks on other systems to direct physical attacks on the system of interest.

1.1.3 Relationship to other technical tasks

Survivability is an integral part of Systems Engineering. .Survivability deals with development and allocation of "survivability" requirements, supports evaluation of options to meet survivability requirements, reoptimizes requirement allocations as necessary, verifies the system meets its survivability requirements, and insures survivability is maintained throughout production and system operational life.

At the highest level, survivability requirements must be defined in terms of system functional performance in a hostile environment which is minimally acceptable to accomplish the mission. These requirements must be translated and allocated as survivability design and verification requirements throughout the system down to the piecepart level. Survivability can be obtained by more means than just physical hardening and for some things the options for physical hardening may be limited or even non-existent. In many cases software rather than hardware solutions may be more effective or development of certain operational procedures may be the most cost effective way to mitigate a threat (e.g., multiple repeats of messages). Survivability as part of Systems Engineering is also responsible for insuring the system requirements are verifiable. System survivability verification is a complex process usually limited technically and, in some cases politically (e.g., nuclear atmospheric and underground tests), limited by threat simulation capabilities and oftentimes limited practically by cost. In order to cover risks associated with uncertainties caused by unknowns in the threat environments themselves, lack of high fidelity threat simulators, limitations in system test capability and analytical methods, and the statistical variations in piecepart or hardware performance, survivability specialists must judiciously incorporate margins into the design and verification requirements flowed throughout the system.

The survivability function closely supports the design process. The survivability function defines requirements (the environments, the acceptable performance envelope, verification method) and provides survivability design guidelines and databases to assist designers in their efforts. Survivability guidelines and associated databases may incorporate piecepart derating data, material shielding guidelines, cable shield effectiveness data, piecepart SEU rates and upset threshold data, current limiting guidelines, etc. Survivability supports the design process in performing trade studies, defining tests, developing survivability models of the system, and performing survivability analyses which will validate system performance. .

There is considerable interaction between Survivability, Reliability, Quality Assurance, and Parts Materials and Processes (PMP). For example, radiation effects must be incorporated into piecepart radiation derating factors and end of life performance data used in worst case circuit analyses, mission life predictions, and system reliability calculations. Survivability provides quality assurance the sampling or screening criteria, test levels, and pass/fail criteria for parts survivability qualification and lot acceptance. Materials and processes must also be reviewed and determined acceptable from a survivability viewpoint (i.e., materials and processes will not undergo unacceptable degradation in the threat environments or cause contamination to sensitive surfaces)..

There is also a close relationship between Survivability and Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC). For example, many of the elements of general good design practice used to protect against the various types of electromagnetic pulse (EMP) share common elements with EMI/EMC or TEMPEST design best practices.

Depending on the requirements and the design approach implemented, survivability can be a significant contributor to the Mass properties of a system. Addition of special shielding, use of heavily shielded cables with terminal protective devices, addition of nulling antennas against jammers are all survivability design approaches which add weight to a system. Survivability can assist in trade studies to reduce weight by evaluating such things as spot (i.e., part) vs. box vs. spacecraft level shielding

Survivability interfaces with Software Engineering and is a major player in Test & Evaluation. Many survivability design features can be partially or totally implemented in software or firmware. Examples may be implementation of error detection and correction (EDAC) schemes to address Single Event Upset or to improve bit error rate performance. System reboot software may be implemented to bring a system back on line after a nuclear radiation induced-circumvention which pulls power from sensitive circuits to prevent burnout. Development testing is at the piecepart, circuit, box, subsystem, and even system level if at all possible. Survivability is properly defined as a set of functional and performance requirements--i.e., the system is to be able to do some specified action within some time under a specified threat (even if it is to be able to shut down during some event and recover full operational capability after some specified time after an event). Therefore, survivability testing should not only be across the widest range of level of assembly possible , but should also include testing at the highest level of assembly practical. Survivability defines the survivability qualification and acceptance test requirements, assists in the selection of test facility, development of test plans and special test equipment, participates in the execution of the test, and post-test analysis. Survivability is a critical area to be addressed during Operational test and evaluation of systems which have survivability requirements against man-made hostile threats. Live Fire Test and Evaluation (LFT&E) is also required by law for certain survivable systems (ref. DoD 5000.2).

Prior to entering production, survivability design must be proven producible. Often during the production phase of a program, Manufacturing Engineering must propose changes either due to parts unavailability, parts obsolescence, or changes to increase efficiency or product yield. The survivability function participates with system and design engineering in evaluating these proposed changes for survivability impacts. Some programs have incorporated special identification and marking of hardness critical items or processes on design drawings as part of their overall hardness assurance efforts. These specially marked drawings can facilitate the change review process and may be used as part of the data base to support Integrated Logistics Support (ILS) planning. The survivability function participates in the ILS process by identifying unique storage and test requirements for satellites as well as developing and implementing hardness maintenance and surveillance programs for survivable ground, sea, and airborne system elements.

Survivability inevitably carries Risk. Threats change as the world changes, reactive threats may be developed to exploit potential vulnerabilities of a system. As the design matures, test and analytical data is received, survivability must continually reassess the system for susceptibilities and vulnerabilities which may jeopardize system survival. Even if threats were static, survivability verification is difficult. Conservative survivability design practice usually must be sacrificed in order to meet or improve system technical performance in other areas and new technologies are introduced into a system with little if any survivability test or evaluation heritage. This increases risk.

1.2 Structure of the Survivability CPAT

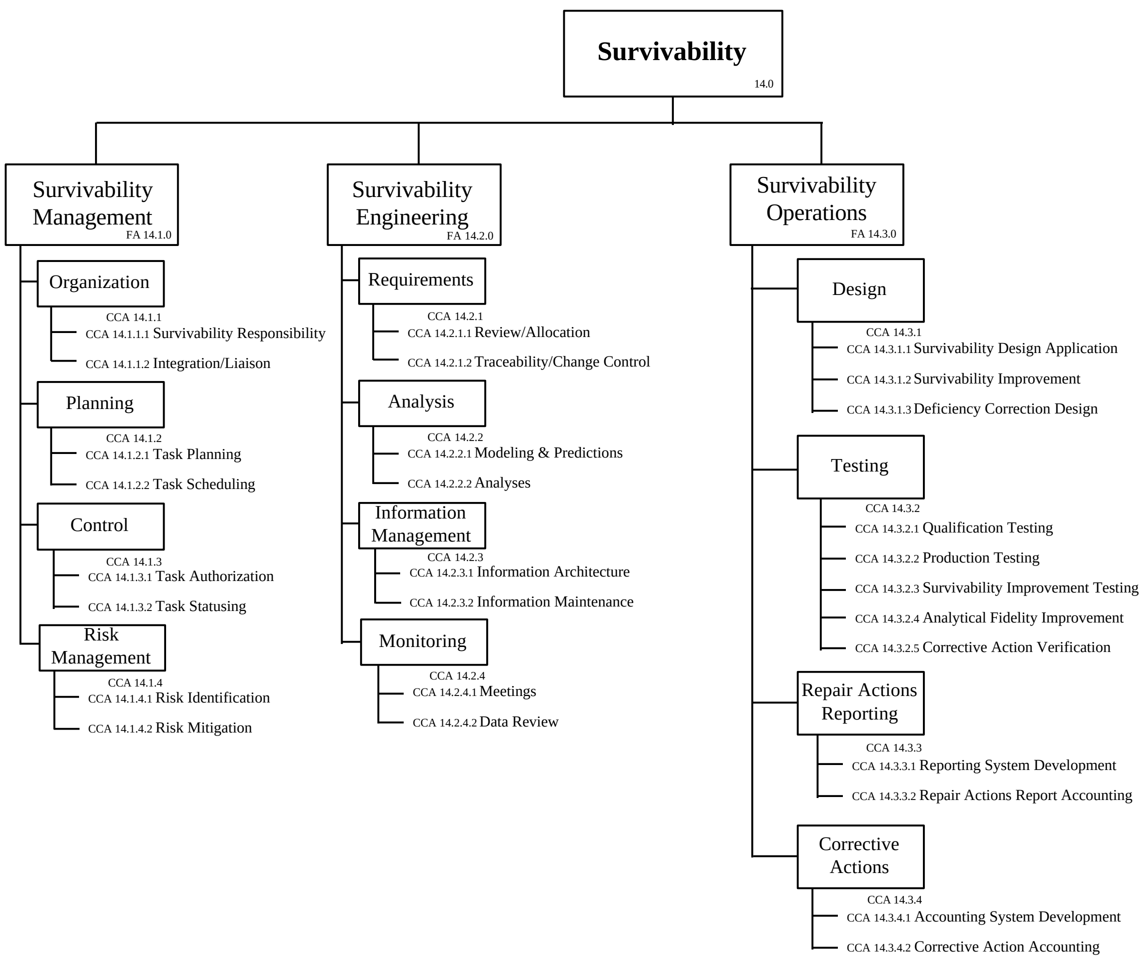
The Critical Process Assessment Tool (CPAT) concept was developed to help SMC System Program Office (SPO) personnel in understanding the functional processes critical to the performance of a program throughout each phase of the acquisition. The CPATs help focus on the critical processes that must be performed within each acquisition phase to ensure that the space system delivered to the government will meet all mission and supportability requirements.

It is the intent of this document to assist the project officer in pre-contract activities such as preparing request for proposal objectives and source selection criteria as well as post-award surveillance of the events in the Integrated Master Plan (IMP).

While Section 1 of this Survivability CPAT document provides general background information regarding the function of survivability in the acquisition process, sections 2 and 3 provide details on the CPAT tool through discussing its application. The general structure of the survivability CPAT discusses generation of the survivability requirements in the systems performance requirements document, identifies survivability critical process objectives as a function of program phase, reviews RFP requirements and source selection criteria to assist in evaluating a proposal in meeting the survivability critical process objectives, and provides detailed criteria and questions for both evaluating proposals as well as monitoring the effectiveness of the contractor's on-going survivability work post contract award. .

Section 2 of this CPAT document which provides potential survivability critical process objectives that may be appropriate for your specific program as well as guidance on RFP instructions/criteria/standards is largely organized by program phase. On the other hand, Section 3 of this CPAT which provides detailed criteria and questions for assisting the project officer or project engineer to evaluate proposals or monitor the effectiveness of a contractor's survivability program is organized to follow the survivability functional flow diagram provided below.

Survivability Management (FA 14.1.0), Survivability Engineering (FA 14.2.0) and Survivability Operations (FA 14.3.0) form the fundamental activities of the survivability function. These three activities are in effect the activities through which survivability work is planned and accomplished. As the survivability functional flow diagram below shows, the three basic survivability functional activities can be broken down further into elements and subelements.. For example,: an element of Survivability Management (FA 14.1.0) is Organization (CCA 14.1.1) which in turn has subelements Survivability Responsibility (CCA 14.1.1.1) and Integration/Liason (CCA 14.1.1.2). Section 3, "Detailed CPAT Criteria and Questions", has been structured to parallel the survivability functional flow, with relevant factors/criteria and questions organized by functional activity, element, and subelement.



1.2.1 How to Use the CPAT

This CPAT provides support for implementing and evaluating the survivability function in the acquisition process. Other CPATs provide support in Program Management, Systems Engineering, Risk Management, Logistics, and so on. To use the CPATs, you should first review the separate CPAT Overview, the Program Management CPAT, and then the CPAT(s) in your area(s) of responsibility. You should then merge the data from each CPAT in forming either your inputs to a RFP or the source selection criteria and standards, or, alternatively, to frame questions to consider during either Tech Eval/Fact-finding or contract execution. To prepare the proposal preparation instructions in Section L of the RFP, you (or your SPO or SPO cadre) should start with the Program Management CPAT and then merge in the instructions developed using this CPAT and other relevant CPATs.

Section 1.1.3 of this document (Relationship to other technical tasks) will identify other relevant CPATs which interface with the Survivability CPAT. Because Survivability is an integral part of Systems Engineering, it is strongly recommended the project officers and project engineers responsible for survivability review the Systems Engineering CPAT.

The following table is a road map to this CPAT.

If you want support in the following:	**Then do the following:**
An **overview** of the survivability critical process.	Read Section 1.1 (Description of the Survivability Critical Process) while referring to the *Concepts & Terms* in Appendix A for unfamiliar terms. Then refer to the *Applicable Documents* listed in Appendix B.
Determine if survivability is a critical process for an up-coming contract.	Survivability is a critical process for all systems/item development, modification, or off-the-shelf acquisition since survivability requirements must be determined and verified.
Prepare the survivability inputs for an **RFP**.	1. Review Section 1 for background. 2. To develop the **Requirements Document**, apply Section 2.1. 3. To develop **survivability objectives** for incorporation into the overall RFP **Statement of Objectives (SOO)**, tailor the objectives in subsection of 2.2 for the program phase you're preparing for. 4. To define **data deliverables** that are pertinent to survivability and are to be required by the RFP, apply Section 2.3. 5. To develop **Proposal Preparation Instructions (PPI)** pertinent to survivability that will be merged with the starting point developed using the Program Management CPAT, apply Section 2.4. 6. To prepare survivability inputs for a **Glossary** for incorporation as attachments to RFP Section J, see Appendix A. 7. To develop **source selection criteria** pertinent to survivability for incorporating into the RFP Section M, apply the subsection of Section 2.4.5 and 2.4.6 for the program phase for which you're preparing.
Prepare survivability inputs to the **source selection standards**.	Tailor the standards in the subsection of Section 2.4.6 for the program phase for which you're preparing.
Prepare for a non-competitive Technical Evaluation (**Tech Eval**) and **Fact-Finding**.	Apply the questions in the subsection of Section 3.1 as they apply to the program phase for which you're preparing.
Maintain **insight** into the contractor's progress in survivability **after contract award**.	Apply the questions in the subsection of Section 3.1 as they apply to your program phase.

1.2.2 Concepts and Definitions.

See Appendix A.

1.2.3 Applicable Documents

See Appendix B.

1.2.4 Additional Support

Contact the SMC AXMP staff office (310) 363-2406 for additional support and the latest policy in the functional area covered by this CPAT module.

Section 2.0 RFP Support

The previous section provided an introduction to the survivability process for defense acquisition programs as a prelude to providing specific support to project officers and project engineers in preparing critical process objectives and Requests for Proposal (RFP) requirements.

2.1 System Performance Requirements Document or Other Requirements Document

The requirements that the system hardware and/or software must meet are defined by the government in the contract in a system functional or performance specification or other requirements document such as a Functional, System, or Technical Requirements Document (FRD, SRD, or TRD). The requirements document is developed by the government or the prime contractor(s) using the system engineering process. The resulting document can be formatted following Data Item Description (DID) DI-IPSC-81431, System/Subsystem Specification (SSS), or the prime contractor(s) may be required to draft it in accordance with the Contract Data Requirements List (CDRL) using the DID tailored to the procurement.

Top level system specifications define survivability in terms of:

1. The natural conditions and threats a system is to withstand
2. The associated threat scenarios
3. The free field environments representing the hostile natural conditions and the threats
4. The functional performance expected of the system when subjected to the natural environment and each threat or threat scenario for
    a. Trans-attack, and
    b. Post-attack
5. The requirements for verifying compliance to survivability requirements
6. The requirements for maintaining the survivability of the system during production, over the storage and operational life of the system.

This list forms the components of what in combination defines the survivability requirements for a system. Development of the survivability requirements should, therefore, involve concurrent consideration of all these factors.

Threats must be based on Defense Intelligence Agency (DIA) validated documents which provide threat projections over the time period the system is expected to be deployed and operational. Threats can be direct attacks on the system of interest or the result of collateral effects due to attacks on other nearby systems. A Mission Need Statement (MNS) may give a general description of the threat or expected levels of conflict for which the needed military capability must be provided. Threats, threat scenarios, and the system performance expected trans and post-attack are iteratively defined and refined as concept, cost, and military effectiveness and utility studies are performed. These studies support development of the Operational Requirements Document (ORD) initially prepared by the user or user representative by Milestone I and further refined at later stages of a program which presents results of mission area analyses in terms of military utility (capability provided in meeting the mission need as stated in the MNS) and cost effectiveness. The ORD will provide minimum acceptable threat levels a system must perform in (thresholds) and goals (objectives). The survivability requirements identified in the System Specifications are traceable to the ORD and at a minimum must provide the threshold capabilities stated in the ORD. The System Specifications are based on further cost and utility analyses of a general concept or concepts and provide additional refinements and detail in threat and threat scenario definition as well as the associated required system performance.

Threat descriptions provided in the System Specification must include the key characteristics of a hostile entity that provides or contributes to its lethality. For example, key characteristics of a weapon or weapons system would include pointing or targeting accuracy if applicable. A nuclear weapons threat against a system ground element (e.g., a user terminal, or control station) must include the nuclear weapons type, the yield (e.g., megatons), the height of burst, and the delivery accuracy (circular error probability, or CEP).

Threat scenarios must include relevant threat timeline and spatial information. For example, it is not sufficient to identify only a specific type of RF jammer as a downlink threat. The maximum number of jammers and minimum standoff from a ground terminal must be also be identified. Similarly, for uplink RF jammers, the type, number, and location of jammers must be defined. For ground launched ASAT attacks, the launch trajectory should be identified. Information regarding whether the ASAT was launched in a direct ascent trajectory or Hohmann transfer trajectory when used in combination with the threat characteristics of the ASAT warhead type and the weapon's target acquisition capability (e.g. midcourse correction or terminal homing) provides important threat timeline information. Specifically, this threat scenario information directly impacts the time between attack identification and the time allowable for completion of any evasive action or countermeasure activities. If multiple attacks are possible, the number and timing between attacks should be specified. The system specification should also address whether different types of threats can be applied simultaneously. All these factors affect and drive survivability design.

Information warfare and physical security threats and scenarios are areas that must also be defined in a System Specification. In some cases detailed threat descriptions and scenarios can be provided. In other cases, the specification may define requirements mainly in terms of compliance with various security and system integrity performance requirements such as a) specific TEMPEST, COMSEC, and crypto requirements, b) protection against non-valid users, c) maximum probability of false alarms and false commanding, d) minimum time to penetrate, or e) compliance with standards imposed by the Joint Technical Architecture (JTA) for applicable C4I systems.

Survivability requirements must also translate threats and threat scenarios into what are known as free field environments--i.e., translate threats into their generated hostile environments ignoring any interactive effects with the system. For nuclear weapons the free field environments can be highly complex, are very weapon specific, and the effects dependent on exactly where the nuclear burst is detonated. To first order, neutron fluence, X-ray fluence, total dose, gamma dose rate, and fission debris, are direct weapons products. Interaction of weapons products with the atmosphere, ground, and earth's magnetic field will create additional nuclear weapons free field environments such as electromagnetic pulse, nuclear scintillation, blast, shock, dust, fallout, and thermal environments.

Perhaps one of the most difficult areas in capturing survivability requirements in a system specification is defining what the system functional performance requirements are (i.e., what the system is expected to do and how well or how fast) during and after exposure to the hostile natural or threat environment. Functional performance requirements are stated in terms of a minimum acceptable performance or a maximum acceptable degradation oftentimes with an associated probability (probability of survival or probability of sucess). Defining these requirements requires considerable insight into how this system is to be used and some knowledge of how it interfaces with other systems in providing a mission capability under peacetime conditions and expected levels of conflict. For example, functional requirements can be stated in terms of "operate through", maximum allowable permanent or temporary degradation, and maximum allowable outage with full or partial recovery. Operate through should be defined in terms of mission performance rather than simply as no degradation in system performance (unless necessary). For example, a temporary degradation in a communications link Bit Error Rate (BER) may in effect be transparent to a system user and, could constitute part of an operate through definition. These functional survivability requirements can be significant cost and risk drivers and must be addressed early in the requirements development process (concept studies, mission area analyses, trade studies). Frequently refinements to the functional performance requirements are made as system design evolves.

System specifications must also address survivability verification. For each level of integration (piecepart, component, subsystem, segment, system) and each performance requirement, the verification method must be established. These methods may include test, analysis, inspection, similarity, or some combination of these.

Qualification test levels and acceptance test levels must be defined as well as general piecepart and component hardness assurance (lot acceptance) or screening requirements.

The System Specification should clearly state the requirement to maintain the survivability of the system over the storage and operational life of the system. Further definition of this requirement will identify or constrain storage conditions and limitations as well as formulate the basis for developing the required hardness maintenance and hardness surveillance programs.

Because survivability requirements reveal capabilities, our state of knowledge of weapons technology , or potentially reveal vulnerabilities or susceptibilities to threats the system is not specifically designed to, survivability requirements are usually classified.

2.2 Critical Process Objectives

Prior to the MIL-Specs and Standards Reform, the work requirements for survivability were usually described in a Statement of Work (SOW) task. Now, the policy is to include the government's survivability objectives in an overall government Statement of Objectives (SOO) in the RFP. In response, the contractor proposes a SOW and an Integrated Master Plan (IMP) or equivalent contractual compliance documents in which the contractor defines and commits to using a Survivability process as part of the plan to achieve the objectives stated in the SOO.

The objectives for survivability vary from program phase to program phase. Objectives that apply to each of the program phases are given in the following subsections (2.2.1- 2.2.5). These objectives should be tailored to the specific overall objectives and risks for the contract.

Under some circumstances a glossary or lexicon may be included in the RFP to assist in clarifying terminology used in the Statement of Objectives (SOO) and other sections of an RFP. Because the survivability function is a highly specialized function with unique terminology, it is recommended a glossary be included as an attachment to the RFP.

2.2.1 Objectives for Concept Exploration and Definition (Phase 0)

Obj. 1. Support Systems Engineering in developing survivable system concepts that provide the mission capability identified in the Mission Need Statement (MNS). Examine threats and threat scenarios consistent with the operational capability defined in the MNS and available DIA validated threat documents and develop survivable concepts (including security aspects as appropriate). Concepts should define the top level system architecture, the general survivability approach, the key elements of survivable functionality and performance, and the associated operational concept.

Obj. 2. Perform trade studies within each concept to explore technical alternatives for providing survivability against proposed threats.

Obj. 2.1 Identify operational concept alternatives which provide survivability.

Obj. 2.2 Perform proliferation vs. hardening trades.

Obj. 2.3 Perform maneuvering/mobility vs hardening trades as appropriate..

Obj. 2.4 Perform additional active defense/countermeasure (e.g., chaff, decoys) vs passive defense/countermeasure (e.g., stealth design, anti-jam nulling technology, hardening) trades as appropriate.

Obj. 2.3 Support top level system architecture trades including communications architecture, and orbital configuration which have survivability impacts

Obj. 3. Evaluate each survivable system concept in terms of Military Utility vs. Cost vs. Risk. For the survivability concepts selected for continued development, identify the associated key technologies and risks. Identify risk mitigation approaches for the Program Definition and Risk Reduction (PDRR) phase.

Obj. 4. Provide survivability data and documentation to support decision to enter PDRR.

2.2.2 Objectives for Program Definition and Risk Reduction (PDRR) (Phase I)

Obj. 1. Perform the survivability simulations, technology demonstrations, prototypes development, tests, and/or other risk reduction steps that will provide the basis for Engineering and Manufacturing Development.

Obj. 2. Verify that the survivability concepts (including operational and security aspects as appropriate), technologies, and design approaches can meet the Government's minimum acceptable requirements (thresholds) as stated in the Operational Requirements Document (ORD) and other applicable documents. Provide an evaluation of concept performance against the Government's objective requirements (goals) as stated in the ORD.

Obj. 3. Translate the operational survivability threshold requirements and objectives into a verifiable set of system functional and performance requirements balancing cost, schedule, and risk as a basis for development.

Obj. 4. Provide survivability data and documentation to support decision to enter EMD.

2.2.3 Objectives for Engineering and Manufacturing Development (EMD) (Phase II) including Low Rate Initial Production (LRIP)

Obj. 1. Assist System Engineering in survivability (including security aspects as appropriate) requirement allocations and specification development. Develop the survivability requirements flowdown and allocations throughout the system and its interfaces down to the piecepart level balancing performance, cost, schedule, and risk which will form the basis for design and which can be verified to meet the Government's contractual requirements. Iterate and reoptimize requirement allocations as required.

Obj. 1.1 Translate each threat into a threat environment for each subsystem (satellite , ground terminals, control segment) and allocate survivability functional and performance requirements trans and post attack..

Obj. 1.2 Allocate survivability environment requirements down to the component/piecepart level.

Obj. 1.3 Incorporate margins into design and verification requirements to address uncertainties.

Obj. 1.4 Determine the effect of all environments on all subsystems and components and iterate designs until design is optimized and all performance and survivability requirements are met.

Obj. 2. Perform survivability design trade studies to select a design which optimizes cost, schedule, and risk and which meets the top level specifications.

> **Obj. 2.1** Determine the proper balance between hardening and shielding.
>
> **Obj. 2.2** Determine the proper balance between satellite hardening and maneuvering or other active defensive countermeasures.
>
> **Obj. 2.3** Perform Hardware vs. Software trades for implementing survivability capabilities
>
> **Obj.2.4** Identify operational constraints and requirements associated with survivability design trade alternatives.

Obj. 3. Provide the necessary survivability design guidelines and survivability databases to support detailed design.

Obj. 4. Define and monitor metrics and TPMs to evaluate the performance of the survivability engineering processes and conformance of the evolving design with survivability requirements and cost goals.

Obj. 5. Control change and maintain the survivability functional and design baselines. Inform the government of any changes affecting survivability functional requirements, cost, schedule, or risk before the changes are implemented. Obtain government approval for any changes affecting survivability functional requirements.

Obj. 6. Verify the design meets the Government's survivability (including security aspects as appropriate) requirements.

> **Obj. 6.1** Demonstrate by verification testing, analysis, modeling, or simulation that the design will meet all survivability requirements (including security aspects as appropriate)

Obj. 7. Develop a Hardness Assurance Program which will maintain the survivability of the system through storage and its required operational life. Implement portions of Hardness Assurance Program appropriate to support EMD activities.

> **Obj. 7.1** Develop production screens and acceptance test requirements to ensure the survivability of parts and materials (e.g. lot sampling and latchup screening). Identify higher level of assembly survivability acceptance test requirements.
>
> **Obj. 7.2** Develop production controls and procedures to ensure that survivability is maintained through build, assembly, and test (e.g., identify Hardness Critical Items on drawings, develop special handling and inspection procedures.)
>
> **Obj. 7.3** Develop motivation and awareness training that acquaint production personnel with hardness/survivability critical procedures and processes.
>
> **Obj. 7.4** Develop a Hardness Maintenance and Surveillance Program Plan containing a complete description of survivability maintenance activities for the fielded system including surveillance tests and evaluation activities.

Obj. 8. Ensure operational constraints and procedures critical to survivability design are documented in operator training manuals and user manuals as appropriate.

Obj. 9. Provide survivability data and documentation to support a Low Rate of Initial Production (LRIP) decision or decision to enter production.

2.2.4 Objectives for Production, Fielding/Deployment, and Operational Support (Phase III)

Obj. 1. Ensure survivability of the system (including security aspects as appropriate) is maintained throughout production.

Obj. 1.1. Implement Hardness Assurance Plan.

Obj. 1.2. Ensure proposed changes to manufacturing processes (e.g., to improve efficiency or yield) during production are evaluated for survivability impact before implementation.

Obj. 1.3. Ensure proposed changes to design (e.g., parts changes because of nonavailability) during production are evaluated for survivability impact before implementation.

Obj. 1.4. Provide data and documentation necessary to support Government acceptance

Obj. 2. Implement special storage, handling, and transportation procedures required to insure the survivability of a system is not degraded during fielding and deployment.

Obj. 3. Ensure survivability of the system is maintained throughout system operation.

Obj. 3.1. Implement Hardness Maintenance and surveillance program.

Obj. 3.2. Determine the survivability impacts (including security aspects as appropriate) of any proposed modifications to the operational system before implementation.

Obj. 3.3. Identify potential upgrades or modifications that could increase survivability of the system or facilitate hardness maintenance and surveillance.

2.2.5 Objectives for Demilitarization and Disposal

Obj. 1. Assess impact on survivability (including security aspects as appropriate) of the system as drawdown plans are developed and system components decommissioned.

Obj. 2. Insure classified documents and equipment which established the survivability and security of the system are disposed in a manner consistent with system and national security guidelines.

2.3 Information Deliverables

Data items that the government deems to be essential are usually defined in a Contract Data Requirements List (CDRL) in the RFP. The contractor may propose to deliver additional items in the CDRL or may commit to make them available in the proposed SOW or Integrated Master Plan (IMP), perhaps via an electronic network. Most recent SMC solicitations and contracts require a commitment that the selected contractor(s) deliver data products via a link between the government's and contractor's Management Information System (MIS) or via a contractor-maintained Electronic Bulletin Board (EBB). However handling, storage, and transfer of classified survivability information must comply with all solicitation or contract security and classification guidelines and requirements.

2.3.1 CDRLs and Data Accession List

Data requirements are specified in the Contract Data Requirements List (CDRL) which is an annex to the RFP and usually an Exhibit or Attachment to the Statement of Work (SOW) or other tasking document in the contract. Prior to acquisition reform the detailed requirements for each data item were specified on a DD Form 1423 (or DD Form 1423-1 which can be computer generated). The contents and format were specified in block 4 of the DD 1423 which usually contained a Data Item Description (DID). The DID can serve as a guide to creating a specific data requirements in current procurements.

Current policy is to minimize the number of formal data items required by the contract to those directly required by policy or essential because of program risk. For each data item that is required, it is recommended that the generic requirements usually found in the DID be tailored to the specific requirements, objectives, and risks of the contract. The tailoring is usually specified in Block 16 on the DD Form 1423. In particular, unless otherwise required by law or regulation, it is recommended that the format be tailored to specify that contractor format is acceptable.

For survivability it is recommended that consideration be given to including the data items listed in the table below in the contract requirements. Usually, the survivability deliverables are confined to data items that 1)show how the contractor plans to implement a survivability program 2) document key survivability design analyses which support system verification, 3) provide critical test plans and test reports which support system survivability design verification, 4) provide hardness assurance documentation and production acceptance test reports, and 4) provide the documentation and databases required to implement a hardness maintenance and surveillance program. Survivability requirements will be documented in specifications that the Government may require as deliverables. For programs which require delivery of drawings, hardness critical items or processes may be identified on the drawing in accordance with the hardness assurance plans of the specific program. Of the documents listed, it is recommended that delivery of any specifications to be prepared or updated by the contractor which are to remain under Government control be clearly identified in the contract that results from the RFP.

Table: Survivability-Specific Data Items

Data Item Title	Data Item Description (DID)	Comment
Specifications	See System Engineering CPAT	Survivability requirements are incorporated into all required specification documents
Survivability Program Plan	DI-S-30553	Program plan for conducting survivability function. Identifies organizational interfaces, tasks, and schedules
Survivability Design Analysis and Trade Study Report	DI-S-30554	Documents trade studies and associated survivability design evaluations.

Survivability Design Analysis Report -- System and Subsystem	DI-S-3581/M	Provides evaluation of system and subsystem performance against threat environments. Depending on the threats specified and platform basing these analyses could include: Anti-Jamming performance analysis Low Probability of Intercept (LPI) analysis Nuclear effects link performance analysis System Autonomy analysis TREE analysis Photocurrent burnout analysis Upset analysis SGEMP analysis SEU/SEL analysis IEMP analysis ECEMP analysis Thermomechanical Shock Analysis Operate through analysis Laser Effects Response Analysis HEMP analysis Dynamic response analysis Loads analysis Thermal analysis Laser effects response analysis HPM effects response analysis NBC analysis
Worst Case Circuit Analysis	See Reliability CPAT	Survivability deratings and end of life parameters are incorporated into the design worst case circuit analysis
Radiation Shielding and Ray Trace Model	DI-S-30559/T	Model for evaluating radiation shielding effectiveness and identifying shadowing paths and unshielded lines of sight
Qualification Test Plans	See Test CPAT	General CDRL which can be used to document survivability qualification test plans
Qualification Test Procedures	See Test CPAT	General CDRL which can be used to document survivability qualification test procedures
Qualification Test Reports	See Test CPAT	General CDRL which can be used to document survivability qualification test reports
System Vulnerability Analysis		Provides an assessment of system vulnerabilities and impacts on mission performance
System Security Analysis		Provides an assessment of system performance against security threats
Hardness Assurance Program Plan		Provides plan for maintaining hardness through production. Includes piecepart lot acceptance and screening tests
Acceptance Test Plans	See Test CPAT	General CDRL which can be used to document survivability acceptance test plans
Acceptance Test Procedures	See Test CPAT	General CDRL which can be used to document survivability acceptance test procedures
Acceptance Test Reports	See Test CPAT	General CDRL which can be used to document survivability acceptance test results
Hardness Maintenance and Surveillance Program Plan		Plan for implementing a hardness maintenance and surveillance program

Hardness Maintenance Procedures		Documents the procedures for performing hardness maintenance and identifies associated Tech Orders
Hardness Surveillance Procedures		Documents the procedures for performing hardness surveillance and identifies associated Tech Orders
Technical Interchange Meeting Minutes		A general program CDRL which can be used to document survivability meeting minutes and action items
Survivability Technical Operating Report	DI-S-30559/T	A general CDRL for documenting special survivability studies

2.3.2 Electronic Data Delivery

Most recent SMC solicitations and contracts require that the selected contractor deliver data products via a link between the Government's and contractor's Management Information System (MIS) or via a contractor-maintained Electronic Bulletin Board (EBB). Most of the data items listed in the table above can be obtained in a more timely and useful form via electronic delivery. In addition, the contract need not otherwise specify data items that are generated as part of the offeror's or contractor's system engineering process and that the contractor commits in the SOW or IMP to timely availability through the MIS or EBB. However handling, storage, and transfer of classified survivability information via electronic delivery must comply with all solicitation or contract security and classification guidelines and requirements.

2.4 RFP Requirements (Instructions to Offerors & Evaluation Criteria)

RFP Section L provides instructions to the contractors or offerors for preparing their proposals while RFP Section M provides the criteria against which each proposal will be individually evaluated..

The instructions to the offeror will probably request submittal of a Technical and/or Management Proposal or Presentation, as well as development of the Work Breakdown Structure (WBS), Statement of Work (SOW), Integrated Master Plan (IMP), and Integrated Master Schedule (IMS) using the specified performance/requirements documents and the Statement of Objectives (SOO).

2.4.1 The Technical and/or Management Proposal or Presentation, to the Extent Required by the RFP

Refer to the proposed language for instructions for preparing the technical and/or management proposal provided in the Program Management and System Engineering CPATs. Tailor this language if necessary to clearly encompass the survivability objectives applicable for the acquisition phase of the program (especially if all survivability objectives were not included in the SOO) as well as highlight any unique survivability requirements or constraints your program may have. Survivability may be unique in that the contractor may have to extensively rely on Government Furnished Equipment (GFE)--especially Government provided test facilities, Government Furnished Property (GFP) such as government-developed weapons effects codes, and may require specialized security clearances. These issues must be addressed in the contract.

2.4.2 The Statement Of Work (SOW)

Refer to the proposed language for instructions for preparing the SOW provided in the Program Management and System Engineering CPATs. Tailor this language if necessary to clearly encompass the survivability objectives applicable for the acquisition phase of the program (especially if all survivability objectives were not included in the SOO).

2.4.3 The Integrated Master Plan (IMP)

Refer to the proposed language for instructions for preparing the IMP provided in the Program Management and System Engineering CPATs. Tailor this language if necessary to clearly encompass the survivability objectives applicable for the acquisition phase of the program (especially if all survivability objectives were not included in the SOO) as well as highlight any unique survivability requirements or constraints your program may have. For example, if the contractor's plan assumes availability of Government Furnished Equipment or Property (e.g., access to certain Government-owned survivability test facilities, specialized weapons effects software or data) in order to accomplish the survivability function this must be specifically identified.

2.4.4 The Integrated Master Schedule (IMS)

Refer to the proposed language for instructions for preparing the IMS provided in the Program Management and System Engineering CPATs. Tailor this language if necessary to clearly encompass the key milestones associated with meeting the survivability objectives applicable for the acquisition phase of the program (especially if all survivability objectives were not included in the SOO). If the contractor's plan assumes availability of Government Furnished Equipment or Property (particularly access to certain Government-owned survivability test facilities) the timeframe and duration for access to these Government facilities must be identified to insure there are no conflicts with other programs.

2.4.5 Evaluation Criteria (Section M)

Section M of the RFP provides the bases for contract award. It describes the evaluation criteria, risk assessments, and general considerations that will be used for evaluating each offeror's proposal and selecting one or more contractors for award. Proposals are individually evaluated (i.e., not against each other) against standards established prior to start of proposal evaluation. Refer to the Program Management CPAT for a detailed overview of criteria and standards.

Evaluation criteria include program-specific criteria, assessment criteria, and the cost (or price) criterion. Typically, each program-specific criterion is divided into "areas" and each area further subdivided into "factors", "subfactors", and "elements". How survivability is broken out is highly dependent on the specifics of the individual program. For example, survivability may be an important aspect of the acquisition and identified specifically as an "area" for evaluation. On other programs, survivability may be identified as a "factor" or set of factors, subfactors, and elements under general areas such as system performance and systems engineering.

Section M also sets the relative importance of the criteria and ranks areas and factors relative to the importance to the military customer. Ranking of survivability related areas, factors, and subfactors, and elements will depend on the specifics of an individual program.

Assessment criteria define general categories each performance criteria (area, factor, etc.) will be evaluated in.. "Soundness of approach" is an example of an assessment criteria. Established standards for each assessment criteria are then applied to determine the level of the proposal's acceptability. The program-specific criteria are also evaluated in terms of proposal risk and performance risk.. Again, refer to the detailed overview provided in the Program Management CPAT for additional information.

As was noted earlier, depending on the specific program, survivability may be identified as its own area for evaluation or as a factor under systems engineering or system performance. Regardless of whether survivability is a separate evaluation area or a factor under systems engineering, because of the close relationship of survivability to systems engineering, it is strongly recommended that the Systems Engineering CPAT discussion of factors and standards be reviewed and applied as appropriate to evaluate survivability. Factors for survivability will vary not only by program, but also with program phase. It is, therefore, difficult to provide a list of factors to specifically include in your RFP. If all of your survivability critical process objectives (ref. Section 2.2 of this document) were not included in the SOO, recommend you consider developing factors based on the non-included survivability objectives. Examples of what may be applicable survivability factors or subfactors are given in the following sections. :

2.4.5.1 Factors for Concept Exploration

Examples of survivability factors or subfactors appropriate for concept exploration may be:

Factor 1: Survivability Management
Factor 2: Development of survivability concept(s) and alternatives
Factor 3: Definition of survivability trade studies
Factor 4: Risk identification and proposed mitigation approaches.
Factor 5: Survivability data

2.4.5.2 Factors for Program Definition and Risk Reduction (PDRR)

Examples of survivability factors or subfactors appropriate for PDRR may be:

Factor 1: Survivability Management

Factor 2: Survivability Concept Demonstration
Factor 3: Survivability Requirements Assessment
Factor 4: Survivability Verification Assessment
Factor 5: Survivability Risk
Factor 6: Survivability Data

2.4.5.3 Factors for Engineering and Manufacturing Development (EMD)

Examples of survivability factors or subfactors appropriate for EMD may be:

Factor 1: Survivability Management
Factor 2: Survivability Requirements Allocation
Factor 3: Survivability Trade Studies and Design
Factor 4: Survivability Data
Factor 5: Survivability Metrics
Factor 6: Change Control Impacts to Survivability
Factor 7: Survivability Verification
Factor 8: Hardness Assurance
Factor 9: Operational and Logistical Survivability Constraints
Factor 10: Survivability Risk

2.4.5.4 Factors for Production, Fielding/Deployment, and Operational Support

Examples of survivability factors or subfactors appropriate for production, fielding/deployment, and operational support may be:

Factor 1: Survivability Management
Factor 2: Hardness Maintenance and Hardness Surveillance
Factor 3: Survivability Change Control
Factor 4: Risk identification and proposed mitigation approaches.
Factor 5: Survivability data

2.4.5.5 Factors for Demilitarization and Disposal

Examples of survivability factors or subfactors appropriate for demilitarization and disposal may be:

Factor 1: Survivability Management
Factor 2: Survivability Drawdown Assessment
Factor 3: Risk identification and proposed mitigation approaches.
Factor 4: Survivability data

2.4.6 Source Selection Standards

Once the proposals are received, they are individually evaluated (i.e., proposals are not evaluated against each other) against standards which were formally established prior to source selection. These evaluation standards establish objective measures of what is acceptable for each factor, subfactor, and element when judged against a particular assessment criteria. Typically, assessments against these standards are summarized as blue, green, yellow, or red. Standards are also established to assess proposal risk and performance risk which are usually designated high, medium, or low. Refer to the Program Management CPAT for a detailed discussion on Source Selection Standards.

Each Standard consists of a Header that corresponds to the Area, a Description, and a Criterion or Criteria for each factor The following is suggested as a starting point for preparing standards for survivability.

These standards assume that corresponding suggested standards from the Program Management CPAT as well as CPATs for systems engineering, risk management, logistics support, reliability, and other required specialty disciplines will be considered in preparing for the overall standards for the source selection. In addition, these standards assume that the RFP requires an Integrated Master Plan (IMP) and Integrated Master Schedule (IMS) or the equivalent which include sections which identify survivability related tasks. These suggested standards also assume that the corresponding objectives from Section 2.2 of this CPAT are to be included in the RFP either in the SOO or merged into the factors or assessment criteria in Section M as discussed in subsection 2.4.5. above.

2.4.6.1 Standards for Concept Evaluation

During Concept Evaluation, factors will be assessed against standards which evaluate the offeror's approach and thoroughness in defining alternative survivability concepts to meet the operational requirements, objectively evaluating the proposed concepts, and in identifying the risks associated with each concept.. Standards for Concept Evaluation are presented in conjunction with the applicable survivability factor as follows:

Factor 1: Survivability Management
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability management which meets the requirements of the RFP and which, as a minimum includes

- A clear definition of the relationship of survivability to System Engineering and a process for providing adequate support to System Engineering and the other disciplines.
- Information which supports contractor has the necessary breadth and adequate survivability technical expertise, analytical tools, facilities, and equipment to support SOO objectives and proposed effort.
- Tasks identified in Integrated Master Plan (IMP) and Integrated Master Schedule (IMS) or the equivalent are demonstrated to support meeting the SOO survivability objectives and survivability requirements of the RFP.

Factor 2: Development of survivability concept(s) and alternatives
Standard: The standard is met when the offeror provides a sound, compliant approach for development of survivability concepts and alternatives which meets the requirements of the RFP and other Government documents and which, as a minimum includes

- Definition and commitment to a process for developing survivable concepts against specified threats, threat scenarios, and authorized variations.
- A process which identifies the sensitivity of survivability concept to changes in the threat
- Definition of an adequate concept verification approach and the uncertainities associated with each concept

Factor 3: Definition of survivability trade studies
Standard: The standard is met when the offeror provides a sound, compliant approach for definition of survivability trade studies which meets the requirements of the RFP and other Government documents and which, as a minimum includes

- A process for thorough and objective evaluation of associated cost, schedule, and performance benefits and risks associated with each trade study

Factor 4: Risk identification and proposed mitigation approaches.
Standard: The standard is met when the offeror provides a sound, compliant approach for risk identification and proposed mitigation approaches which meets the requirements of the RFP and other Government documents and which, as a minimum includes

- A thorough and rigorous process for identifying the associated survivability key technologies and risks for each concept proposed.

- A process which adequately identifies survivability risk mitigation approaches for the Program Definition and Risk Reduction (PDRR) phase.

Factor 5: Survivability data
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability data which meets the requirements of the RFP and other Government documents and which, as a minimum includes

- A process for providing survivability data adequate to support and evaluate a concept

- A data management systems which complies with all contract classified information security regulations.

- Identification of information which will be provided to the Government in a timely manner to insure adequate Government insight and allow the Government to perform its oversight function

- A process for establishing a database sufficient to support entering the Program Definition and Risk Reduction (PDRR) phase.

2.4.6.2 Standards for PDRR

During PDRR, factors will be assessed against standards which evaluate the offeror's approach and thoroughness in demonstrating compliance of the proposed design concept(s) with the system survivability requirements; in identifying and proposing risk reduction steps for all the risks that can be mitigated pre-EMD; and in defining the process to be used for survivability demonstration and validation including the identification of simulations, demos, or prototypes for risk reduction. Standards for PDRR are presented in conjunction with the applicable survivability factor as follows:

Factor 1: Survivability Management
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability management which meets the requirements of the RFP and which, as a minimum includes

- A clear definition of the relationship of survivability to System Engineering and a process for providing adequate support to System Engineering and the other disciplines.

- Information which supports contractor has the necessary breadth and adequate survivability technical expertise, analytical tools, facilities, and equipment to support SOO objectives and proposed effort.

- Tasks identified in Integrated Master Plan (IMP) and Integrated Master Schedule (IMS) or the equivalent are demonstrated to support meeting the SOO survivability objectives and survivability requirements of the RFP.

Factor 2: Survivability Concept Demonstration

Standard: The standard is met when the offeror provides a sound, compliant approach for survivability concept demonstration which meets the requirements of the RFP and which, as a minimum includes

- Identification and commitment to performing a set of survivability simulations, technology demonstrations, prototypes development, tests, and/or other risk reduction steps that will adequately and objectively allow concept comparison and selection of a preferred approach or concept alternative

- Identification and commitment to performing a set of survivability simulations, technology demonstrations, prototypes development, tests, and/or other risk reduction steps that will adequately and objectively provide the basis for Engineering and Manufacturing Development.

Factor 3: Survivability Requirements Assessment
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability requirements assessment which meets the requirements of the RFP and which, as a minimum includes

- Identification and commitment to a process which translates the operational survivability threshold requirements and objectives documented in the Government's Operational Requirements Document (ORD) and other applicable documents into a verifiable set of system functional and performance requirements balancing cost, schedule, and risk as a basis for development.

- Identification and commitment to a process which defines driving survivability requirements in terms of cost, schedule, and risk.

Factor 4: Survivability Verification Assessment
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability verification assessment which meets the requirements of the RFP and which, as a minimum includes

- Adequate and objective verification that the survivability concepts (including operational and security aspects as appropriate), technologies, and design approaches can meet the Government's minimum acceptable requirements (thresholds) as stated in the Operational Requirements Document (ORD) and other applicable documents.

- An adequate and objective evaluation of concept performance against the Government's objective requirements (goals) as stated in the ORD and other applicable documents.

- An objective evaluation of the sensitivity of a concept and its alternatives to changes in the threat or threat scenarios and associated uncertainties.

Factor 5: Survivability Risk
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability risk which meets the requirements of the RFP and which, as a minimum includes

- A thorough and rigorous process for identifying the associated survivability technology and verification risks for each concept proposed and translating these risks in terms of cost, schedule, and performance impact.

- A process which adequately identifies survivability risk mitigation approaches and trades for the EMD phase.

Factor 6: Survivability Data

Standard: The standard is met when the offeror provides a sound, compliant approach for survivability data which meets the requirements of the RFP and which, as a minimum includes

- A process for providing survivability data adequate to objectively support and evaluate a concept
- A data management systems which complies with all contract classified information security regulations.
- Identification of information which will be provided to the Government in a timely manner to insure adequate Government insight and allow the Government to perform its oversight function
- A process for establishing a database sufficient to support entering the EMD phase.

2.4.6.3 Standards for EMD

During EMD, factors will be assessed against standards which evaluate the offeror's approach and thoroughness in demonstrating compliance of the proposed design with the survivability requirements, and in demonstrating survivability can be maintained throughout production and over the life of the system. Standards for EMD are presented in conjunction with the applicable survivability factor as follows:

Factor 1: Survivability Management
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability management which meets the requirements of the RFP and which, as a minimum includes

- A clear definition of the relationship of survivability to System Engineering, Design Engineering, Test, System Effectiveness, EMC/TEMPEST, Quality Assurance, Logistics, Production and other disciplines and a process which identifies and commits to providing adequate support to these disciplines.
- Information which supports contractor has the necessary breadth and adequate survivability technical expertise, analytical tools, facilities, and equipment to support SOO objectives and proposed effort.
- Tasks identified in Integrated Master Plan (IMP) and Integrated Master Schedule (IMS) or the equivalent are demonstrated to support meeting the SOO survivability objectives and survivability requirements of the RFP.

Factor 2: Survivability Requirements Allocation
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability requirements allocation which meets the requirements of the RFP and which, as a minimum includes

- Identification and commitment to a process to assist System Engineering in survivability (including security aspects as appropriate) requirement allocations and specification development. Process will identify development of the survivability requirements flowdown and allocations throughout the system and its interfaces down to the piecepart level balancing performance, cost, schedule, and risk which will form the basis for design and which can be verified to meet the Government's contractual requirements.
- Process will allow for iteration and reoptimization of requirement allocations as required.

- A process for translation of each threat into a threat environment for each subsystem (satellite , ground terminals, control segment) and allocation of survivability functional and performance requirements trans and post attack..

- A process for incorporating adequate margins into design and verification requirements to address uncertainties.

Factor 3: Survivability Trade Studies and Design
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability trade studies and Design which meets the requirements of the RFP and which, as a minimum includes

- Performance of sufficient survivability design trade studies to select a design which objectively optimizes cost, schedule, and risk and which meets the top level specifications.
- Defining and committing to a process which determines the effect of all environments on all subsystems and components and iterates designs until design is optimized and all performance and survivability requirements are met.
- Defining and committing to a process which identifies the driving survivability requirements in the system and relates the performance of the proposed design approach to those requirements. Provides test, demonstration, or analytical data that are, in turn, based on test or demonstration data of the key technologies to adequately and objectively support the soundness of a proposed design.
- Defining a process which determines the proper balance between hardening and shielding as appropriate.
- Defining a process which determines the proper balance between satellite hardening and maneuvering or other active defensive countermeasures as appropriate.
- Commitment to performing Hardware vs. Software trades for implementing survivability capabilities as appropriate.
- Description of a process to provide sufficient survivability development test and design analyses to support design decisions at major Government/contractor design reviews.
- Identification of operational constraints and requirements associated with survivability design trade alternatives.
- A description and commitment to a process which provides survivability support to design and system engineering both in-house and with subcontractor's and vendors during evolving design.
- A description and commitment to a process that continually evaluates the performance, cost, schedule, and risk of the evolving design. For any changes affecting functional performance requirements (including external interfaces), cost, delivery, or risks the contractor describes and commits to a process that will provide timely notification and adequate information (including description, impacts, and justification) for a timely decision by the government.

Factor 4: Survivability Data
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability data which meets the requirements of the RFP and which, as a minimum includes

- A process for providing survivability data adequate to objectively support and evaluate a design.
- A data management systems which complies with all contract classified information security regulations.

- Identification of information which will be provided to the Government in a timely manner to insure adequate Government insight and allow the Government to perform its oversight function

- A process for providing the necessary survivability design guidelines and survivability databases to adequately support detailed design.

- A process for providing survivability data and documentation to adequately and objectively support a Low Rate of Initial Production (LRIP) decision or decision to enter production.

Factor 5: Survivability Metrics
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability metrics which meets the requirements of the RFP and which, as a minimum includes

- Definition and commitment to a process which defines and monitors metrics and Technical Performance Measures (TPMs) to evaluate the performance of the survivability engineering processes and conformance of the evolving design with survivability requirements and cost goals.

- Description of a process and commitment to the periodic evaluation of metrics that indicate the extent to which the survivability process is in control and ready for completion of the next event. Describes and commits to the periodic evaluation of TPMs that indicate the degree to which adequate technical performance is being achieved.

Factor 6: Change Control Impacts to Survivability
Standard: The standard is met when the offeror provides a sound, compliant approach for change control impacts to survivability which meets the requirements of the RFP and which, as a minimum includes

- Definition and commitment to a process for controlling change, determining the impact of change, and maintaining the survivability functional and design baselines.
- A process which informs the government of any changes affecting survivability functional requirements, cost, schedule, or risk in a timely manner before the changes are implemented

Factor 7: Survivability Verification
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability verification which meets the requirements of the RFP and which, as a minimum includes

- Description and commitment to a sound survivability verification program which adequately demonstrates design compliance to the Government's requirements throughout the system's required life cycle through the appropriate mixture of test, analysis, modeling, and/or simulation.

- Test program which encompasses the widest range of levels of integration and assembly as is meaningful and culminates in tests at the highest level of integration and assembly as is practical.

- A survivability verification process which adequately addresses threat and threat environment simulation uncertainties.

- Description of and commitment to a process to successfully accomplish Live Fire Test and Evaluation (if applicable).

- Commitment to a process which ensures availability of sufficient design verification test and analytical data to support Initial Operational Test and Evaluation (IOT&E) planning by an independent agency.

Factor 8: Hardness Assurance
Standard: The standard is met when the offeror provides a sound, compliant approach for hardness assurance which meets the requirements of the RFP and which, as a minimum includes

- Description and commitment to the development of a Hardness Assurance process which ensures the design is producible and that system will meet all survivability requirements through follow-on production. Description should include identification of portions of a Hardness Assurance Program appropriate to support EMD activities.

- Development of and commitment to a process for defining production screens and acceptance test requirements to ensure the survivability of parts and materials (e.g. lot sampling and latchup screening). Process shall include identification of higher level of assembly survivability acceptance test requirements for production as appropriate.

- Development of and commitment to a process for defining production controls and procedures to ensure that survivability is maintained through build, assembly, and test (e.g., identification of Hardness Critical Items on drawings, develop special handling and inspection procedures.)

- Development and commitment to motivation and awareness training that acquaintsproduction personnel with hardness/survivability critical procedures and processes.

- Definition of a process and commitment to developing a Hardness Maintenance and Surveillance Program Plan containing a complete description of survivability maintenance activities for the fielded system including surveillance tests and evaluation activities.

Factor 9: Operational and Logistical Survivability Constraints
Standard: The standard is met when the offeror provides a sound, compliant approach for operational and logistical survivability constraints which meets the requirements of the RFP and which, as a minimum includes

- A process for ensuring operational constraints and procedures critical to survivability design are documented in operator training manuals and user manuals as appropriate.

- Description and commitment to a process for developing storage, deployment, and Hardness Maintenance, and Hardness Surveillance plans which maintain operational survivability.

Factor 10: Survivability Risk
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability risk which meets the requirements of the RFP and which, as a minimum includes

- A thorough and rigorous process for identifying survivability cost, schedule, performance risks in a timely manner and raising to the appropriate level of Government and contractor oversight for risk mitigation or resolution.

- A thorough and rigorous process for identifying survivability technology, design, verification, and production risks translating these risks in terms of cost, schedule, and performance impact.

- Commitment to a process which tracks risk resolution at a level of oversight and frequency appropriate.

- A process which adequately identifies survivability risk mitigation approaches and trades for the production, deployment, and operational support phase.

2.4.6.4 Standards for Production, Deployment, Operational Support

a. Production: During Production, factors will be assessed against standards which evaluate the offeror's approach and thoroughness in the process to be used for survivability including completing or maintaining the product baseline, evaluating proposed process or design changes for survivability impacts, and maintaining all data bases. Standards for Production are presented in conjunction with the applicable survivability factor as follows:

Factor 1: Survivability Management
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability management which meets the requirements of the RFP and which, as a minimum includes

- A clear definition of the relationship of survivability to System Engineering and a process for providing adequate support to System Engineering, Manufacturing, Quality Assurance and the other disciplines.
- Information which supports contractor has the necessary breadth and adequate survivability technical expertise, analytical tools, facilities, and equipment to support SOO objectives and proposed effort.
- Tasks identified in Integrated Master Plan (IMP) and Integrated Master Schedule (IMS) or the equivalent are demonstrated to support meeting the SOO survivability objectives and survivability requirements of the RFP.

Factor 2: Hardness Assurance
Standard: The standard is met when the offeror provides a sound, compliant approach for hardness assurance which meets the requirements of the RFP and other Government documents and which, as a minimum includes

- A description and commitment to a process for implementing an adequate hardness assurance plan to ensure system survivability is maintained throughout production
- A description and commitment to a process for actively monitoring production processing to ensure timely identification and correction of loss of production controls
- Commitment to performing end item hardness acceptance tests as needed

Factor 3: Survivability Change Control
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability change control which meets the requirements of the RFP and other Government documents and which, as a minimum includes

- A description and commitment to a process for ensuring survivability is not compromised during proposed changes to production for manufacturing process improvements
- A description and commitment to a process for ensuring survivability is not compromised during proposed changes to production because of part or material obsolescence.

Factor 4: Risk identification and proposed mitigation approaches.
Standard: The standard is met when the offeror provides a sound, compliant approach for risk identification and proposed mitigation approaches which meets the requirements of the RFP and other Government documents and which, as a minimum includes

- A thorough and rigorous process for identifying survivability risks during production and assessing impacts in terms of cost, schedule, performance.

- A process which adequately identifies survivability risk mitigation approaches and actively monitors progress to resolution.

Factor 5: Survivability data
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability data which meets the requirements of the RFP and other Government documents and which, as a minimum includes

- A process for providing survivability data adequate to support and evaluate maintenance of the production baseline

- Identification of information which will be provided to the Government in a timely manner to insure adequate Government insight and allow the Government to perform its oversight function
- A data management systems which complies with all contract classified information security regulations.

- A process for establishing a database sufficient to support deployed system Hardness Maintenance and Surveillance

b. Fielding/Deployment and Operational Support : During Fielding/Deployment and Operational Support, factors will be assessed against standards which evaluate the offeror's approach and thoroughness in the process to be used for maintaining survivability through storage, transport, fielding, and operations. Standards for Fielding/Deployment and Operational Support are presented in conjunction with the applicable survivability factor as follows:

Factor 1: Survivability Management
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability management which meets the requirements of the RFP and which, as a minimum includes

- A clear definition of the relationship of survivability to System Engineering and Logistics and a process for providing adequate support to System Engineering, Logistics and the other disciplines.
- Information which supports contractor has the necessary breadth and adequate survivability technical expertise, analytical tools, facilities, and equipment to support SOO objectives and proposed effort.
- Tasks identified in Integrated Master Plan (IMP) and Integrated Master Schedule (IMS) or the equivalent are demonstrated to support meeting the SOO survivability objectives and survivability requirements of the RFP.

Factor 2: Hardness Maintenance and Hardness Surveillance
Standard: The standard is met when the offeror provides a sound, compliant approach for hardness maintenance and surveillance which meets the requirements of the RFP and other Government documents and which, as a minimum includes

- A description and commitment to a process for implementing an adequate hardness maintenance and surveillance plan to ensure system survivability is maintained throughout storage, transportation, deployment, and operations.
- A description and commitment to a process for actively monitoring hardness maintenance and surveillance problems and activities to verify program adequacy or the need for program changes.

Factor 3: Survivability Change Control
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability change control which meets the requirements of the RFP and other Government documents and which, as a minimum includes

- A description and commitment to a process for ensuring survivability is not compromised during proposed changes to improve operations or logistics
- A description and commitment to a process for ensuring survivability is not compromised during proposed changes to logistical or maintenance support because of part or material obsolescence.

Factor 4: Risk identification and proposed mitigation approaches.
Standard: The standard is met when the offeror provides a sound, compliant approach for risk identification and proposed mitigation approaches which meets the requirements of the RFP and other Government documents and which, as a minimum includes

- Commitment to and description of a thorough and rigorous process for identifying survivability risks during storage, transportation, deployment, and operations and assessing impacts in terms of cost, schedule, performance.
- A process which adequately identifies survivability risk mitigation approaches and actively monitors progress to resolution.

Factor 5: Survivability data
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability data which meets the requirements of the RFP and other Government documents and which, as a minimum includes

- A process for providing survivability data sufficient to support and evaluate storage, transport, deployment, and operational procedures and activities have not compromised survivability.
- Identification of information which will be provided to the Government in a timely manner to insure adequate Government insight and allow the Government to perform its oversight function
- A data management systems which complies with all contract classified information security regulations.
- A process for establishing a database sufficient to support modification or upgrade programs as necessary.

2.4.6.5 Standards for Decommissioning/Disposal

During Decommissioning/Disposal, factors will be assessed against standards which evaluate the offeror's approach and thoroughness in the process to be used for survivability including any changes which affect survivability such as changes in operational capabilities of the system if decommissioning is incrementally accomplished (i.e., to provide some limited capability as new systems are fielded or to support transition plans for new systems), updates to the disposal data and plans, any design, manufacture, and/or coding necessary to complete the required disposal actions, as well as handling/disposal of classified information and equipment Standards for Decommissioning/Disposal are presented in conjunction with the applicable survivability factor as follows:

Factor 1: Survivability Management
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability management which meets the requirements of the RFP and which, as a minimum includes

- A clear definition of the relationship of survivability to System Engineering and a process for providing adequate support to System Engineering and the other disciplines as needed.
- Information which supports contractor has the necessary breadth and adequate survivability technical expertise, analytical tools, facilities, and equipment to support SOO objectives and proposed effort.
- Tasks identified in Integrated Master Plan (IMP) and Integrated Master Schedule (IMS) or the equivalent are demonstrated to support meeting the SOO survivability objectives and survivability requirements of the RFP.

Factor 2: Survivability Drawdown Assessment
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability drawdown assessment which meets the requirements of the RFP and other Government documents and which, as a minimum includes

- A description and commitment to a process for adequately and objectively assessing the impact on survivability of the system as drawdown plans are developed and system components decommissioned.

Factor 3: Risk identification and proposed mitigation approaches.
Standard: The standard is met when the offeror provides a sound, compliant approach for risk identification and proposed mitigation approaches which meets the requirements of the RFP and other Government documents and which, as a minimum includes

- Commitment to and description of a thorough and rigorous process for identifying survivability risks during decommissioning/disposal.
- A process which adequately identifies survivability risk mitigation approaches and actively monitors progress to resolution.

Factor 4: Survivability data
Standard: The standard is met when the offeror provides a sound, compliant approach for survivability data which meets the requirements of the RFP and other Government documents and which, as a minimum includes

- A process for providing survivability data sufficient to support and evaluate decommissioning/disposal procedures and activities have not compromised survivability beyond what is allowable.

- Identification of information which will be provided to the Government in a timely manner to insure adequate Government insight and allow the Government to perform its oversight function

- A data management systems which complies with all contract classified information security regulations.

- Description of and commitment to a process that ensures classified documents, software and data storage media, and equipment which established the survivability and security of the system are disposed in a manner consistent with contract and national security guidelines.

3.0 Detailed CPAT Criteria and Questions

Section 3. Detailed CPAT Criteria and Questions

The critical process evaluation method applied in this CPAT has, in part, been adapted from that used in AFMC Pamphlet 63-103, 15 June 1994, *Software Development Capability Evaluation*. The purpose is to effectively evaluate the contractor's survivability technical and management capabilities before contract award and during contract execution.

3.1 Technical Evaluation (Tech Eval)/Fact-finding Review Questions

Upon receipt of the proposal, you will begin an analysis of the effort, approach, and costs that relate to survivability and probably a number of other areas as well. This thorough technical evaluation of the proposal is an essential first step. Following this initial review, you will likely need the opportunity to (1) obtain a full understanding of your area(s) of the proposal, (2) identify areas requiring clarification or more detail, and (3) discuss with the contractor your specific areas of concern. This "Fact-Finding" is usually accomplished at the contractor's facility. Your role as a technical evaluator of specialized areas is to provide a comprehensive and substantiated evaluation for the technical evaluator team lead. (You may also happen to be the team lead.)

You will summarize your findings for inclusion into the *Technical Evaluation Report*. This report will form a basis for negotiations. (See the Program Management and System Engineering CPATs for recommended elements of a technical evaluation.)

- Summarize the proposed effort, unique costs, unique technical aspects, and risks
- Summarize the proposed hours.
- Summarize your recommended hours
- Explain your disallowed hours -- establish sound, well documented technical justification.

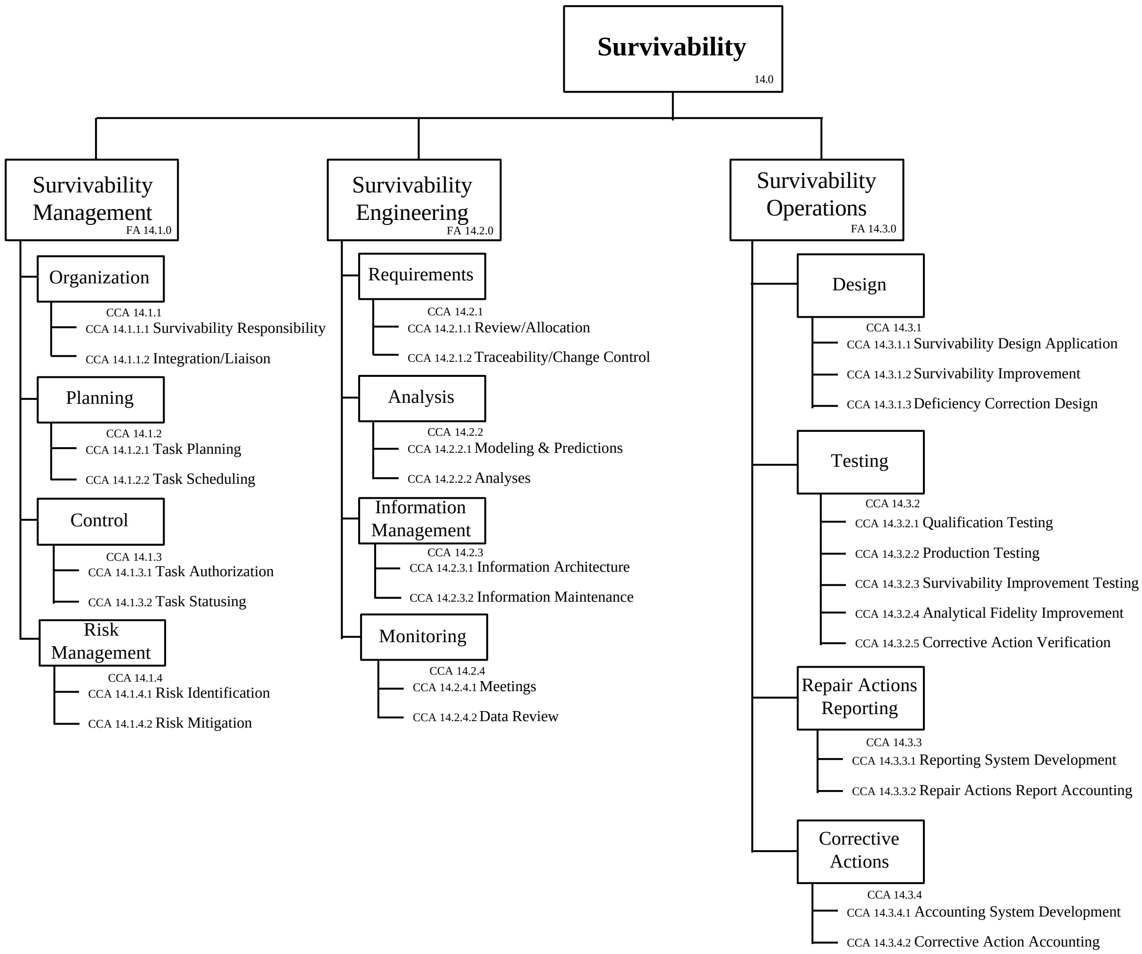
Often a range of reasonableness is established with highs and lows. The highs denote minimal risk to the contractor and lows assume greater risks to the contractor. However, we need to also consider technical and schedule risks to the government and the contractor. These technical and schedule risk considerations include such things as design complexity, design stability, prior experience, etc.. Of course, risk mitigation goes hand-in-hand with the appropriate mix of survivability studies, analyses, tests, demos and how the results are applied to the design, development, and production of the proposed system or item.

3.1.1 Tech Eval/Fact-finding Review Questions for Concept Exploration, PDRR, EMD, Production, Operational Support, and Decommissioning/Disposal

The technical analysis, fact-finding, and technical report will usually consume a significant amount of your time. The approaches to evaluating and preparing for contractor selection and negotiations vary. The common thread in this process is the evaluation of the proposal against Section L of the RFP, Proposal Prep Instructions. This includes the SOO which you had referenced in Section L.

The critical process evaluation method applied in this CPAT has in part, been adapted from that used in AFMC Pamphlet 630103, 15 June 1994, Software Development Capability Evaluation. The purpose is to effectively evaluate the survivability aspects of a contractor's engineering and management capabilities before contract award and during contract execution. The Functional Areas, Critical Capabilities, and Questions tend to be generic in nature and are intended to identify typical capabilities, capacities, and questions for successful development and production of mission critical systems.

The general structure of this section follows the survivability functional flow diagram shown in the figure below with relevant factors/criteria and questions listed for each of the 14.X.X.X sub elements. The reader may use the survivability function flow diagram (or its tabular listing also provided below) as an index to find the required critical process and the level of detail required for the task at hand.



Survivability Function-- Tabular listing

FA 14.0 Survivability Management

- **CCA 14.1.1 Organization**
  - **CCA 14.1.1.1 Survivability Responsibility**
  - **CCA 14.1.1.2 Integration/Liason**
- **CCA 14.1.2 Planning**
  - **CCA 14.1.2.1 Task Planning**
  - **CCA 14.1.2.2 Task Scheduling**
- **CCA 14.1.3 Control**
  - **CCA 14.1.3.1 Task Authorization**
  - **CCA 14.1.3.2 Task Statusing**
- **CCA 14.1.4 Risk Management**
  - **CCA 14.1.4.1 Risk Identification**
  - **CCA 14.1.4.2 Risk Mitigation**

FA 14.2.0 Survivability Engineering

- **CCA 14.2.1 Requirements**
  - **CCA 14.2.1.1 Review/Allocation**
  - **CCA 14.2.1.2 Traceability/Change Control**
- **CCA 14.2.2 Analysis**
  - **CCA 14.2.2.1 Modeling and Predictions**
  - **CCA 14.2.2.2 Analyses**
- **CCA 14.2.3 Information Management**
  - **CCA 14.2.3.1 Information Architecture**
  - **CCA 14.2.3.2 Information Maintenance**
- **CCA 14.2.4 Monitoring**
  - **CCA 14.2.4.1 Meetings**
  - **CCA 14.2.4.2 Data Review**

Survivability Function Tabular Listing (Cont.)

FA 14.3.0 Survivability Operations

- **CCA 14.3.1 Design**
  - **CCA 14.3.1.1 Survivability Design Application**
  - **CCA 14.3.1.2 Survivability Improvement**
  - **14.3.1.3 Deficiency Correction Design**
- **CCA 14.3.2 Testing**
  - **CCA 14.3.2.1 Qualification Testing**
  - **CCA 14.3.2.2 Production Testing**
  - **CCA 14.3.2.3 Survivability Improvement Testing**
  - **CCA 14.3.2.4 Analytical Fidelity Improvement**
  - **CCA 14.3.2.5 Corrective Action Verification**
- **CCA 14.3.3 Feedback Reporting**
  - **CCA 14.3.3.1 Reporting System Development**
  - **CCA 14.3.3.2 Report Accounting**
- **CCA 14.3.4 Corrective Actions**
  - **CCA 14.3.4.1 Accounting System Development**
  - **CCA 14.3.4.2 Corrective Action Accounting**

FA 14.1.0 Survivability MANAGEMENT

CCA 14.1.1 Organization

CCA 14.1.1.1 Survivability Responsibility

C1. The offeror's organizational structure clearly identifies a Survivability focal point responsible for meeting overall program survivability objectives as well as defines lines of authority and accountability for each element within the organizational structure. **(Q1, Q3)**
C2. The total Survivability organization is defined with elements which encompass program survivability objectives and provide support compatible with the program's Work Breakdown Structure (WBS). **(Q2, Q4)**
C3. All internal interfaces within the survivability organization have been defined and responsibilities for information exchange and coordination clearly established. **(Q5, Q6, Q7)**
C4. Required resources (e.g. Survivability specialists, methods, tools) are integrated into the program organizational working structure. **(Q8, Q9)**
C5. The Survivability program stays technically current with the broader Government and civilian technical communities in terms of relevant data, analytical and testing techniques and can make adjustments as necessary. **(Q10)**

Q1. Is there a clearly defined survivability focal point identified in the organizational structure who is responsible for defining and overseeing a survivability program which meets overall program survivability objectives and insures a well balanced and fully integrated program? **(C1)**

Q2. Is a Survivability organizational structure completely defined with responsibilities assigned to each element in the organization which encompass the overall program survivability objectives? **(C2)**

Q3. Have lines of authority and accountability been clearly established within each element of the survivability organization and are they consistent with the overall program organizational structure? **(C1)**

Q4. Are survivability organizational responsibilities defined such that they support the appropriate processes, services, and products identified in the contract's Work Breakdown Structure (WBS) of the program? **(C2)**

Q5. Have requirements for coordination between internal survivability organizational elements been defined and a process for surfacing and resolving technical issues identified? **(C3)**

Q6. Does each element of the survivability organization know what data or other products or services it is responsible for providing to other elements within the survivability organization? **(C3)**

Q7. Does each element of the survivability organization know what data or other products or services it is responsible for providing to organizations external to the survivability organization? **(C3)**

Q8. Do survivability personnel have appropriate technical qualifications and experience? **(C4)**

Q9. How is the organization structured to meet the program needs for specialized technology skills which may or may not be required full time? **(C4)**
For example,

- Are survivability specialists program dedicated personnel so there is no issue of responsibility, availability, and program continuity, or,
- Are survivability specialists pulled as required from non-program specific corporate functional groups so there may be issues of responsibility, availability and program continuity. If so, how are issues related to availability, and program continuity resolved? or
- Are the survivability specialized skills provided by subcontractors? If so, how are issues related to responsibility, authority, availability, and program continuity resolved?

Q10. How does the survivability organization insure its data, analysis techniques, and test techniques stay current with the general practices and standards of the broader technical community? **(C5)**

- Are there corporate resources which allow key survivability team members to participate in technical and scientific conferences? Are major technical journals and databases available?

FA 14.1.0 Survivability MANAGEMENT
CCA 14.1.1 Organization
CCA 14.1.1.2 Integration/Liason

C1. The integration of Survivability into project operations is defined including the interfaces between the Survivability organization and all other program organizations necessary to meet all survivability objectives. **(Q1, Q2, Q3, Q4, Q5)**
C2. Contractor-to-Government interface(s) have been identified to coordinate and work on survivability related matters. **(Q4, Q6)**
C3. All Contractor-to-Contractor (i.e., contractor A to contractor B) responsibilities have been identified as appropriate. **(Q4, Q6)**
C4. The methods and responsible individuals for monitoring and evaluating the Survivability program compliance are documented. **(Q4, Q5)**
C5. Methods for working survivability interface issues, recording actions, and implementing resolutions are defined. **(Q6)**

Q1. Have organizational responsibilities and lines of authority and accountability been clearly defined across contractor internal program interfaces? **(C1)**
For example,

- Has the role of survivability as part of Systems Engineering been defined?
- Has the interface of Survivability with Quality and Design Assurance been defined?
- Has the interface of Survivability with all Product Design organizations been defined?
- Has the interface of Survivability with Test been defined?

Q2. Have lines of authority clearly been established in situations where contractor cross-functional organizations are responsible for executing portions of the survivability program? **(C1)**
For example,

- Have roles and responsibilities been clearly defined between Survivability and Quality/Design Assurance for insuring the parts program is consistent and compliant with survivability requirements?
- Has the role and authority of Survivability in supporting the Parts, Material, and Processes Board (PMPCB) been established?
- Has the role and authority of Survivability in supporting other specialized functional areas which may be designated to execute portions of the survivability program (e.g., Mechanical and Thermal Design) been established?
-

Q3. Has the interface of Survivability with all subcontractors and vendors been defined? **(C1)**

Q4. Does each element of the survivability organization know what data or other products or services it is responsible for providing to organizations external to the survivability organization and when each is required? **(C1, C2, C3, C4)**
For example,

- What survivability data, products, and/or services are required to support other program organizations such as Design, Quality Assurance, Test?
- What survivability data, products, and/or services are required to support subcontractors and vendors?

- What survivability data, products, and/or services are required to support other contractors who share a system interface?
- What survivability data, products, and/or services are required to support Government activities?

Q5. Who is responsible and what method is proposed and documented for verification and monitoring Survivability Program compliance internally, for subcontractors/vendors, and contractor-to-contractor interfaces as appropriate? **(C1, C3, C4)**

Q6. How are survivability issues surfaced, and actions and their resolutions documented and tracked for contractor program internal, contractor-to-subcontractor/vendor, contractor-to-contractor, and contractor-to-government interfaces? **(C1, C2, C3, C5)**

FA 14.1.0 Survivability MANAGEMENT
CCA 14.1.2 Planning
CCA 14.1.2.1 Task Planning

C1. The tasks to be performed are identified and defined and consistent with the program's overall survivability objectives, contract requirements, and the contract Work Breakdown Structure (WBS). **(Q1, Q2, Q4, Q6, Q7, Q8, Q18)**
C2. Task planning and definition factors in realistic resource requirements (budget, manpower, equipment, etc.) necessary to sustain the program and support all program contract milestones and program schedules. **(Q10, Q11, Q12, A13, Q14, Q15, Q16, Q18)**
C3. Tasks are defined in a manner consistent with the program's cost and schedule control accounting system. **(Q3)**
C4. Tasks encompass all data, product, and services support required across all program interfaces. **(Q5, Q6, Q8, Q18, Q19)**
C5. There is a process for timely review of task progress, and internal reallocation of resources as required. **(Q17, Q18)**

Q1. Have tasks been defined which will allow all program survivability objectives to be met and are consistent with the program's system engineering objectives? **(C1)**

Q2. Can tasks be correlated to the contract Work Breakdown Structure? **(C1)**

Q3. Have tasks been broken down into individual work packages for program cost and program schedule progress monitoring/auditing (CPR or CSSR)? **(C3)**

Q4. Have tasks been identified and defined which support the appropriate contract hardware, software, and documentation or data deliverables? **(C1)**

Q5. Are survivability tasks defined which correlate to all data, product, or services needs across all organizational interfaces? **(C4)**

Q6. Have the tasks associated with meeting the program's survivability objectives been identified and documented in a Survivability Management Plan, Survivability Program Plan and/or other specific documents? **(C1, C4)**

Q7. Are survivability program plans consistent with the Program's Master Plan and the System Engineering Master Plan (SEMP)? **(C1, C4)**

Q8. Are subcontractor survivability plans consistent with the contractor's survivability plan? **(C1, C4)**

Q9. Is an OPR (office of primary responsibility) assigned to each task? Are all performing, contributing, or coordinating survivability organizational elements or other organizations identified with each task? Have all organizations committed to these tasks? **(C4)**

Q10. Have tasks been sufficiently defined to allow realistic resource estimates and estimates for task completion? **(C2)**

Q11. Has the Survivability program been allocated adequate resources to implement and sustain the program through completion? **(C2)**

- Have the full time and shared resources (manpower, equipment, classified storage facilities etc.)been considered?
- How are shared resources allocated and availability issues resolved between other programs?

Q12. Have Lessons Learned been factored into task planning and resource estimates? **(C2)**

Q13. How are resource estimates generated for Survivability, what is the historical accuracy of the estimates, and how are they to be validated? **(C2)**

Q14. How are the manpower loading estimates for Survivability activities developed and what assures that each of the tasks required for Survivability program implementation (e.g., requirements definition, analysis, documentation, design and manufacturing support, subcontractor and vendor support , test, management, and control etc.) are included in the estimates? **(C2)**

Q15. How are the needs for the required specialty skills developed and what is their make-up over the entire program life cycle? **(C2)**

Q16. Do personnel have the appropriate security clearances to perform the tasks assigned? **(C2)**

Q17. How is task progress monitored and is there a process for reallocating resources if necessary? **(C5)**

Q18. Are reviews for technical accuracy and sufficiency included in task plans? **(C1, C2, C4, C5)**

Q19. Is support to appropriate technical interchange meetings, program reviews, interface control working groups, Parts, Material, and Processes Control Board, Engineering Change Board, Failure Review Board, etc., identified in task plans? **(C4)**

FA 14.1.0 Survivability MANAGEMENT
CCA 14.1.2 Planning
CCA 14.1.2.2 Task Scheduling

C1. The timing of required survivability tasks and their relationship to other tasks and operations is defined and consistent with overall program schedules and milestones. **(Q1, Q2, Q4, Q5, Q9, Q10, Q11)**
C2. Task schedules are realistic and current. **(Q3, Q9, Q11)**
C3. Schedule uncertainty and risk are considered in schedule planning. **(Q6, Q7)**
C4. All required test facilities and long lead items have been identified and scheduled. **(Q8, Q9))**

Q1. Are schedules consistent with the program's Integrated Master Schedule (IMS)? **(C1)**

Q2. Is the time phasing of tasks consistent with task interrelationships (i.e., how one task feeds into another) and with meeting the overall program schedules? **(C1)**

Q3. Are the impacts of survivability task progress and current schedule information incorporated in reports on overall program schedule status and plans? **(C2)**

Q4. Is the timing of required Survivability tasks and their relationship to other tasks and operations defined? **(C1)**

Q5. Are schedules incorporated into and consistent with the program's cost/schedule performance baseline? **(C1)**

Q6. Is schedule uncertainty estimated and what is the basis of the estimate? (**C3)**

Q7. What margin is built into the schedule and what is the probability of the project exceeding the allotted time including margin? **(C3)**

Q8. Have all required external test facilities been identified and scheduled? **(C4)**

Q9. Have all long lead items been identified and scheduled? **(C1, C2, C4)**

Q10. Are task schedules consistent with GFE, and GFI availability? **(C1)**

Q11. Are task schedules consistent with associated subcontractor or vendor schedules? **(C1, C2)**

FA 14.1.0 Survivability MANAGEMENT
CCA 14.1.3 Control
CCA 14.1.3.1 Task Authorization

C1. Controls are in place so that survivability work remains within contract scope and resources are effectively utilized. **(Q1, Q2, Q4)**
C2. Task authorizations are issued against the proper cost account. **(Q3)**

Q1. How will work be authorized and who provides the authorization? **(C1)**

Q2. Who reviews task to ensure task is within contract scope? **(C1)**

Q3. How are cost accounts assigned to task authorizations? **(C2)**

Q4. Are task authorizations issued with a specified period of performance or limitation of hours? If not, how are expenditures controlled? **(C1)**

FA 14.1.0 Survivability MANAGEMENT
CCA 14.1.3 Control
CCA 14.1.3.2 Task Statusing

C1. Task progress and status are tracked at the appropriate management levels with the corresponding detail and frequency to insure issues are surfaced, impacts identified, resolutions defined, and corrective actions implemented in a timely and effective manner. **(Q1, Q2, Q3, Q4)**
C2. Progress and status of Survivability tasks assigned to other functional organizations and subcontractors is provided in sufficient detail and frequently enough to assist Survivability Management in identifying issues and implementing corrective actions in a timely and effective manner. **(Q2, Q3, Q4)**
C3. There is adequate survivability technical oversight and review of survivability work in progress and products to insure tasks are being performed correctly. **(Q5, Q6)**

Q1. How does Program Management track survivability program status? What information is tracked and how frequently? **(C1)**

Q2. How does Survivability Management track survivability program status? What information is tracked and how frequently? **(C2)**

Q3. Which organization has the responsibility of ensuring the Survivability issues are resolved expeditiously and with minimum impact to the program? **(C1, C2)**

Q4. How are subcontractor related efforts tracked? What information is provided to survivability management and how frequently? **(C1, C2)**

Q5. What level of technical oversight is provided by Survivability to other organizations and subcontractors assigned to perform survivability-related tasks? **(C3)**

Q6. Is there an established review process for evaluating adequacy and correctness of survivability work in progress and completed tasks as well as compliance with program requirements? **(C3)**

FA 14.1.0 Survivability MANAGEMENT
CCA 14.1.4 Risk Management
CCA 14.1.4.1 Risk Identification

C1. Internal procedures are identified for survivability risk identification, and tracking/statusing of issues until resolution. **(Q1, Q2, Q5)**
C2. There is a process for alerting Program Management and the Government of risks and potential impacts in a timely manner. **(Q2, Q3, Q4)**
C3. Clear criteria or measures have been established to assist in recognizing program risks. (Q9)
C4. Risks are quantified in terms of probability of occurrence or probability of failure and program impact (cost, schedule, technical). **(Q6, Q7, Q8, Q10)**

Q1. What internal procedures are identified for risk identification and tracking/statusing of issues until resolution? **(C1)**

Q2. Who is responsible for identifying survivability risk? **(C2)**

Q3. How is Program Management made aware of survivability related risks and how are risks monitored for potential program impact? **(C2)**

Q4. How is the Government made aware of survivability related risks and kept informed on potential program impact? **(C2)**

Q5. How is the Survivability Manager or organizational Survivability focal point made aware of survivability related risks and how are risks monitored for potential program impact? **(C1)**

Q6. How is the impact to the program identified and quantified? **(C4)**

Q7. How is a probability of occurrence or probability of failure determined for a specific risk? **(C4)**

Q8. If appropriate, does the survivability risk assessment quantify the impact in terms of degradation in military utility? Does the risk depend on enemy knowledge of the inability of the system to meet its specified survivability requirements or knowledge of an identified system susceptibility? **(C4)**

Q9. Are clear criteria or measures established to recognize something as a potential program risk? Specifically, are there cost, schedule and technical risk criteria established? **(C3)**

- Are there any technical performance measures (TPMs) related to survivability which will be routinely monitored?

Q10. Has survivability risk been a factor considered in design or verification approach decisions? **(C4)**

FA 14.1.0 Survivability MANAGEMENT
CCA 14.1.4 Risk Management
CCA 14.1.4.2 Risk Mitigation

C1. Risk mitigation planning is recognized as a key management responsibility for ensuring a technically sound, and cost effective program. **(Q1, Q5)**
C2. Risk mitigation plans are developed for each risk with clear decision points identified for implementation. **(Q2, Q3)**
C3. There are procedures for monitoring the progress of risk items, implementation of the risk mitigation plan, and integration with the overall program. **(Q4)**

Q1. Is Survivability risk mitigation planning identified as a specific function or task in the Survivability Management Plan, Program plan, and System Engineering Management Plan (SEMP)? **(C1)**

Q2. Have risk mitigation plans been developed for each risk identified? **(C2)**

Q3. Do risk mitigation plans include clear decision points when certain actions must be taken to minimize overall program impact? **(C2)**

Q4. Are there procedures for monitoring the progress of risk items, implementation of the risk mitigation plan, and integration with overall project effort? **(C3)**

Q5. Has risk mitigation been considered in requirements allocation, survivability design development and manufacture, verification, and lifecycle maintenance? **(C1)**

FA 14.2.0 Survivability ENGINEERING

CCA 14.2.1 Requirements

CCA 14.2.1.1 Review/Allocation

C1. Survivability requirements allocation has been incorporated into the overall systems engineering requirements allocation process. **(Q1, Q3, Q4, Q5, Q7, Q8)**
C2. The survivability requirements allocation process preserves the integrity of the system in meeting its survivability performance and functional requirements and provides a basis for a robust survivability design. **(Q3, Q4, Q6, Q7, Q8)**
C3. Allocated survivability requirements are traceable down to the piece part level and requirements are verifiable at each level of integration. **(Q4, Q6, Q10, Q13, Q14)**
C4. The Survivability requirements allocation process explicitly factors in the uncertainties in translating system level threats and threat scenarios to a set of derived environments. **(Q9, Q11)**
C5. Derived requirements and associated design margins are self-consistent and balanced. **(Q11, Q12)**
C6. Threats are derived from the System Threat Assessment Report (STAR) or other DIA validated documents and are traceable to the Operational Requirements Document. **(Q2, Q15)**

Q1. How has the survivability requirements allocation process been integrated into the overall system engineering requirements allocation process? **(C1)**

Q2. Have all threats (including manmade weapons, natural environment, and security threats) and threat scenarios been sufficiently defined? **(C6)**
For example,

- Have all key weapons parameters been defined (e.g., peak power, pulse width, duty cycle, jitter, frequency, modulation, etc.)
- Have key platform and support systems information been defined which can affect weapon effectiveness (e.g., mobile or fixed platform, weapon pointing accuracy, surveillance and targeting capabilities including target identification accuracy and target positioning accuracies, ASAT launch locations and trajectory type)
- Has the key scenario information been defined (e.g., number of jammers, location of jammers, height of burst, location and timing of bursts in an attack, timing between attacks.)

Q3. Have specific system performance and functional requirements been defined for system operations trans and post threat attack? **(C1, C2)**

Q4. In keeping with survivability as a system engineering discipline, are survivability requirements allocations traceable not only by segment, configuration item, component, and across interfaces, but traceable by system function as well? **(C1, C2, C3)**

Q5. What trades have been considered in developing a survivability requirements allocation and what are the associated survivability risks and program risks (cost, schedule, technical)? **(C1)**
For example,

- Are there intersegment or intrasegment trades that can be made?
- Are there physical hardening vs. proliferation trades that can be made?
- Are there physical hardening vs. operations trades that can be made (e.g., maneuver, active or passive defense)?

- Are there Hardware vs. Software trades?

Q6. How does integration of Government Furnished Equipment (GFE), Non Developmental Items (NDI), or Commercial Off-the-Shelf (COTS) impact the requirements allocation? **(C2, C3)**

Q7. Is the allocation of survivability requirements consistent with the system operational concept including the role and limitation of humans in systems operations? **(C1, C2)**

Q8. While allocations may support the system requirement, are there any inherent system susceptibilities that may potentially be exploited because of the way the requirements have been allocated? Can the susceptibility be mitigated or eliminated? **(C1, C2)**

Q9. Have threats been translated into the appropriate free field environments at the location (s) of interest (e.g., at the satellite, ground terminal, or control station)? **(C4)**
For example,

- For the natural space environment have the earth's natural trapped radiation, cosmic ray and solar flare, micrometeorite and debris, and natural ionospheric scintillation and absorption environments been defined?
- For a nuclear burst have the gamma ray, X-ray, neutron, and fission product dose/decay rates and dose profiles been determined; have the Electromagnetic Pulse (EMP), nuclear scintillation, blast, shock, thermal, fallout and dust environments been determined as appropriate?
- For lasers, High Power Microwave weapons, and jammers have energy deposition rates, and power density spectral profiles been defined?

Q10. Have transport and coupling codes been used to translate free field environments into system design to environments? **(C3)**
For example, for spacebased systems exposed to a nuclear weapons environment,

- Have radiation transport calculations been performed to derive transient and total dose radiation environments at the box and component level?
- Have thermomechanical shock requirements been derived?
- Have SGEMP, IEMP, and ECEMP requirements been derived?

Q11. Are design margins incorporated into the allocated margins to account for uncertainties in the following: **(C4, C5)**

- Uncertainties in the environment predictions?
- Component performance variabilities?
- Limitations in verification methods (test and analysis)

Q12. Are derived weapons effects environments balanced? For example for a ground terminal, the radiation effects environments are consistent with the blast and shock requirements for a specified megaton bomb which bursts x feet away. **(C5)**

Q13. Are all requirements verifiable and have the means of verification been identified? **(C3)**

Q14. Do the verification requirements at increasing levels of integration provide an cohesive, and integrated approach to supporting verification of survivability performance and functional requirements at the system level? **(C3)**

Q15. Are all threats based on DIA validated documents and is there traceability to the system's operational requirements document (ORD)? **(C6)**

- Is there a System Threat Assessment Report (STAR) and is it current?

FA 14.2.0 Survivability ENGINEERING
CCA 14.2.1 Requirements
CCA 14.2.1.1 Traceability/Change Control

C1. System requirements are traceable to the operational requirements document (ORD) objectives and thresholds. **(Q1)**
C2. Survivability is integrated into the System Engineering process and as such all Survivability Functional, Performance, and Verification Requirements allocated from the system down to the piecepart level have full traceability to the Government specified system requirements. **(Q2)**
C3. Survivability design requirements are baselined and maintained under configuration control. **(Q3)**
C4. Design (drawings, associated data/documentation) is baselined and maintained under configuration control. **(Q4, Q5)**
C5. Changes are evaluated for survivability impacts prior to implementation. **(Q6, Q8)**
C6. Exception processing is evaluated for survivability impacts prior to approval. **(Q7)**

Q1. Are system survivability requirements traceable to the objectives and thresholds of the Operational Requirements Document? **(C1)**

Q2. Has full traceability (i.e., top-down and bottom-up) of derived and allocated survivability requirements been demonstrated? How? **(C2)**

- Have requirements flow diagrams been developed and documented?
- How have these diagrams been reviewed and assessed for completeness and accuracy?

Q3. How are survivability requirements baselined and put under configuration control? **(C3)**

- Who signs off in survivability to verify requirements are correct and accurately represent the baseline?

Q4. What survivability documentation is maintained under configuration control? **(C4)**

- Are contractor developed Survivability Design Guidelines maintained under configuration control?
- What survivability databases are maintained under configuration control?
- Are there any survivability or related system models maintained under configuration control?

Q5. How does Survivability coordinate on baseline design drawings and databases? Does Survivability formally sign-off on documentation and drawings that are put under configuration control? **(C4)**

Q6. Are proposed changes evaluated for survivability impacts before implementation? **(C5)**

- Are proposed design changes evaluated by survivability?
- Are proposed manufacturing process changes evaluated by survivability?

Q7. All exception processing in terms of PMP actions must be evaluated for survivability impact prior to approval and documented. **(C6)**

For example, survivability should evaluate the impact of

- Sample size deviations for radiation testing
- Deviations from established piecepart pass/fail test criteria
- New materials proposed to be added to the approved parts and material list.

Q8. How is the Survivability organization incorporated into the change process? **(C5)**

- Does Survivability have a formal seat on the Engineering Change Board or Configuration Control Board?
- Does Survivability assist in determining whether a proposed change constitutes a Class I (requires Government approval) or Class II (does not require Government approval) change?

FA 14.2.0 Survivability ENGINEERING
CCA 14.2.2 Analysis
CCA 14.2.2.1 Modeling & Predictions

C1. The contractor has the analysis and modeling capability to translate threats and threat scenarios into survivability design requirements. **(Q1, Q2, Q3)**
C2. Analytical and modeling capability exists to support system trade studies. **(Q2, Q7, Q8, Q9, Q10)**
C3. There are analytical tools and supporting databases to develop survivability Design Guidelines for Engineering teams during design development. **(Q5)**
C4. There exist the analytical tools and supporting databases to model the system to sufficient fidelity to accurately predict system survivability performance and quantify uncertainties. **(Q6, Q7, Q8, Q9, Q10, Q12)**
C5. Survivability models and predictions are updated as design is iterated. **(Q11)**
C6. Survivability models have been validated or there is a plan for performing validation. **(Q3, Q4)**
C7. There is an interaction between analyses and tests used to verify system survivability performance--i.e., one feeds into the other. **(Q12, Q14)**
C8. There is an analytical capability to support test planning and post-test performance evaluation. **(Q13)**

Q1. In order to begin the survivability requirements definition and allocation process, does the contractor have threat models and analytical tools for translating threats and threat scenarios into free-field environments at the location of interest? **(C1)**

- Is there the capability to model single threat environments?
- Have appropriate synergies been considered in multiple threat scenarios?

Q2. To assist in the survivability requirements allocation process does the contractor have the appropriate transport and coupling codes to model environment-system interactions and calculate derived environments and their associated effects as appropriate? **(C1, C2)**
For example, depending on the specified threats and whether a system is space or ground based,

- Are there radiation transport codes?
- Are there analytical tools for defining SGEMP, IEMP, and ECEMP levels?
- Are there High Altitude burst EMP (HEMP) and Dispersed EMP (DEMP) coupling codes?
- Are there Source Region (SREMP) EMP coupling codes?
- Are there analytical tools for predicting thermomechanical shock levels?
- Are there analytical tools for predicting material outgassing?
- Are there codes for predicting blast and shock wave coupling and deriving expected loads and accelerations?
- Are there laser, RF, and microwave irradiation coupling models?

Q3. Have all threat and threat environment models and codes been validated? **(C1, C6)**

- Are nuclear effects models/codes obtained from the Defense Nuclear Agency?
- Are codes obtained from the Air Force Weapons Laboratory?
- Are Nuclear environments obtained from the Nuclear Criteria Group?

Q4. How will system-specific models be validated? **(C6)**

- What test data will be used to help validate the models?

Q5. Does Survivability have the databases and modeling capability to issue a Survivability Design Guidelines document to design engineers to assist in design development? **(C3)**
For example,

- Does this design guideline give component derating and end of life information?
- Does this design guideline give methodologies and databases for predicting upset and burnout?
- Does this design guideline give SGEMP responses of various cable types?
- Does this design guideline give radiation shielding effectiveness information for various materials?

Q6. Are there analytical tools and data bases available to develop models for predicting component and circuit level responses? **(C4)**

- Models and databases for predicting upset or burnout due to dose rate effects?
- Models and databases for predicting upset or burnout due to EMP?
- Models and databases for predicting cumulative dose effects?
- Models and databases for predicting component latchup due to prompt dose effects?
- Models for predicting upset or latchup due to Solar Flare and Cosmic Ray events?
- Models and databases for predicting mechanical response?
- Models and databases for predicting thermomechanical response?
- Models and databases for predicting RF induced upset or burnout.
- Models and databases for predicting surface responses to dust, debris, or micrometeorites?
- Models and databases for predicting responses of circumvention and recovery circuitry?

Q7. Are there system models to evaluate system functional performance against threat environments and threat scenarios both trans and post-attack? **(C2, C4)**
For example,

- Total dose effect on satellite system performance and ability to meet survivability functional performance and lifetime requirements?
- SEU rate effect on mission data bit error rate?
- Laser irradiation effect on payload sensor outage/false target detection?
- Jammer effects on communications performance?
- Natural and nuclear threat-induced absorption and scintillation effects on communication performance?
- Dust effects on communications and mission performance?
- Debris gamma effect on sensor false target detection rate and impact on system performance?
- Cold X-ray induced optics distortion effect on sensor resolution/sensitivity and impact on system performance?
- System transient radiation effects response and functional performance

Q8. Does the contractor have the capability to assess system performance and survivability against various Security threats? **(C2, C4)**

- Can the contractor evaluate system performance against specified physical security threats (sabotage)?
- Can the contractor evaluate system performance for COMSEC and TEMPEST security?
- Can the contractor evaluate the capability of the system against unauthorized users or penetration by computer hackers?
- Can the contractor evaluate the capability of the system against software Trojan Horse threats or viruses?

Q9. Does the contractor have the capability to accurately assess System autonomy capabilities during hostilities? **(C2, C4)**

Q10. Does the contractor have the analytical tools and models to predict system performance of Active and/or Passive defense systems? **(C2, C4)**
For example,

- Effectiveness of satellite maneuver strategies against ASAT threats and impacts on system performance?
    - Impacts of maneuver (e.g., effects of acceleration on satellite dynamics, effects of maneuver propellant contamination) on system mission performance?
    - Detailed end-game analysis--e.g., ASAT target acquisition and homing via maneuver signature?
- Effectiveness of various decoys and decoy strategies and impacts on system mission performance?
    - Decoy discrimination via maneuver signature?
    - Decoy discrimination via plume impingement acceleration?

Q11. Are survivability models and analyses kept current and updated as design is iterated? **(C5)**

- Are system models maintained under configuration control?

Q12. Are test data used to refined models and reduce model uncertainties? **(C4, C7)**

Q13. What analyses are needed to support test planning (including test set up) and post test performance evaluations? **(C8)**

Q14. What portions of survivability design validation (i.e., demonstration that the design meets all survivability requirements) will be accomplished by analysis? **(C7)**

- What associated system models are needed?
- What tests support these analyses?
- How do analyses support verification tests?

FA 14.2.0 Survivability ENGINEERING
CCA 14.2.2 Analysis
CCA 14.2.2.2 Analyses

C1. Adequate analytical tools exist for supporting evolving design process. **(Q1, Q2, Q3, Q4)**
C2. Adequate databases exist or are obtained to support analytical efforts. **(Q8)**
C3. Uncertainties have been appropriately factored into analytical results. **(Q5, Q6)**
C4. Analyses have been independently reviewed for correctness and adequacy. **(Q10)**
C5. Analyses support identification of risk areas and areas for test. **(Q6)**
C6. Analyses support test planning, pre-test predictions, and post-test performance evaluation. **(Q7)**
C7. System survivability must ultimately be verified by analysis; there is sufficient test and analytical data at the piecepart to system level to support system verification. **(Q5)**
C8. Analyses support system susceptibility and vulnerability assessments. **(Q9)**

Q1. What analyses will be performed to support the requirements allocation process? **(C1)**
Are they analytical tools recognized by the technical community, for example:

- Defense Nuclear Agency?
- Air Force Weapons Laboratory?
- National Security Agency?
- Joint Electronic Warfare Center?

Q2. Are there analyses to support development of a Survivability Design Guidelines for product engineers? **(C1)**

Q3. What survivability analyses will be used to support trade studies? **(C1)**

Q4. What analyses will be used to support survivability design evaluations during development? **(C1)**
For example, will there be a

- Shielding Analysis
- Worst Case Circuit Analysis
- Transient Radiation Effects Analysis (burnout and upset)
- SGEMP, IEMP, ECEMP analysis
- EMP analysis (upset and burnout)
- Blast and shock dynamic response analyses
- Thermal effects analysis
- Anti-jamming analysis
- Laser effects analysis
- Low Probability of Intercept performance analysis
- Microwave and RF upset and burnout analyses
- Nuclear effects on link performance analyses (scintillation, absorption)
- SEU analysis
- System timing analysis
- Operate through analysis
- Circumvention Recovery Analysis
- Maneuver effectiveness analysis

- System Physical Security Analysis
- System Software Security Analysis
- System TEMPEST and COMSEC analyses
- System OPSEC analysis
- Probability of Find or Detection Analysis
- System Autonomy analysis

Q5. How will analysis be used to support system survivability verification? **(C3, C7)**

- What test data (piecepart, circuit, box, subsystem, configuration item, segment, system) is required to support the analysis?
- What information is required for Non Developmental Items (NDI), Commercial Off-the-Shelf (COTS) or Government Furnished Equipment (GFE) incorporated into the system for system verification?
- What lowered tiered analyses will be used to support the system verification analysis?
- Will system analysis evaluate functional capability trans and post attack?
- What are the uncertainties in this analysis and how are they mitigated?
- How is a system level minimum Probability of Survival (or maximum allowed Probability of Failure) requirement verified?

Q6. How has analysis been used to identify areas of high risk or uncertainty? **(C3, C5)**

- How will the risks or uncertainties be mitigated? Will risks be mitigated through testing or design changes?

Q7. What analytical support is required for test? **(C6)**

- What analysis has been used to support test planning and pre-test predictions?
- What analysis has been used to support post test performance evaluations?

Q8. What databases are required to support analytical efforts? **(C2)**

- Are there historical databases which have adequate documentation to verify their accuracy and applicability?
- What tests will have to be specifically performed to obtain the necessary databases?

Q9. What analysis methods will be used to perform a system vulnerability analysis? **(C8)**

- What characterization data is required to support this analysis?
- Will fragility curves be obtained on sensitive or suspected low damage threshold components?

Q10. What is the independent analytical review process to insure analyses are accurate and sufficient? **(C4)**

- Who reviews the analyses? Are they survivability specialists?
- How is independence maintained?
- Whose signatures are required for approval and release?

FA 14.2.0 Survivability ENGINEERING
CCA 14.2.3 Information Management
CCA 14.2.3.1 Information Architecture

C1. The type of information (data/documents) required both contractually and internally has been identified. **(Q1, Q2, Q3, Q4)**
C2. The interrelationships between the identified data/documents has been identified and hierarchies established. **(Q5)**
C3. The interrelationships between data/documents and key program events, milestones, reviews, audits, and tests is identified. **(Q6)**
C4. Changes to one piece of the information architecture are appropriately flowed through information in the remaining architecture. **(Q7, Q8)**

Q1. What contract deliverables (CDRLs) are Survivability related or require Survivability inputs? **(C1)**

- Are there program plans?
- Are there requirements documents, specifications, interface control documents?
- Are there Survivability Design Analysis reports?
- Are there design review packages?
- Are there survivability test plans and procedures?
- Are there survivability test reports?
- Are there survivability technical operating reports to document special studies?
- Are drawings a contract deliverable?
- Are there meeting minutes?
- Are there Failure Analysis Reports which may require Survivability support?
- Are Hardness Maintenance/Hardness Surveillance Plans and procedures required?
- Is a Hardness Assurance Plan required?
- Are Hardness Assurance Test Data documents required to be formally submitted to the Government either directly by contract requirement or through Parts, Material, and Processes Board (PMPCB) action?

Q2. What information data/documents is Survivability required to generate for internal program use--i.e., what information have other organizations identified they need to perform their function or that Survivability has identified as necessary to support their role to provide technical assistance, audit or evaluate other organizations' survivability related efforts? **(C1)**

- Has Survivability prepared a Survivability Design Guideline with databases and best-practices information to assist product engineering during design development?
- Has Survivability provided radiation deratings and end of life information to product engineering and Reliability/Design Assurance?
- Has Survivability provided piecepart characterization test requirements and lot qualification and acceptance test requirements (including pass/fail criteria) to Quality Assurance?
- Has Survivability established material and process guidelines?
- Has Survivability established packaging guidelines?
- Has Survivability provided technical information to the Test organization for test planning and execution?

- Has Survivability provided Subcontractors and Vendors necessary information to assist in their design development or production efforts which insures consistency with contractor internal efforts?
- Has Survivability provided Cost and Schedule information and status to Program Control?
- Has Survivability provided necessary analysis, requirements, test, risk information to System Engineering?
- Has Survivability provided necessary program status, manpower, issues information to Program management?

Q3. What information data/documents does Survivability require from other contractor organizations to perform the survivability function? **(C1)**

- What information (technical, schedule) does Survivability need from System Engineering?
- What information (technical, schedule) does Survivability need from product (hardware and software) engineering?
- What information (technical, schedule) does Survivability need from Test? Characterization test data, fragility data, qualification test data, acceptance test data?
- What information (technical, schedule) does Survivability need from Quality Assurance?
- What information (technical, schedule)does Survivability need from the Subcontractors and Vendors?

Q4. What information data/documents does Survivability require from organizations external to the contractor's organization? **(C1)**

- What information does Survivability need from the Government (e.g., source threat documents, data on GFE, Government analytical models, Government test data, operational information)? Is this information on the GFI list of the contract?
- What information does Survivability need from another contractor regarding an interface?

Q5. Has the contractor defined the interrelationships between data and documentation as well as a hierarchical architecture? **(C2)**
For instance,

- Is there a Specification Tree?
- Is there a drawing tree?
- Are there Verification Cross Reference Matrices (VCRMs) or some equivalent established within each specification which correlate requirements to verification method and an overall Survivability verification plan which explains how tests and analyses support each other?

Q6. Has the documentation required to support program milestones been identified? **(C3)**

- What survivability documentation is required to support a SDR, PDR, CDR, MRR, or other program review?
- What survivability documentation is required to support Functional Configuration Audit and the Physical Configuration Audit (FCA/PCA)?

Q7. What information (documentation/databases) are maintained under configuration control? **(C4)**

Q8. What process is there to flow changes in databases, changes in information provided in documents, or requirements changes to other databases/documentation that may be affected? **(C4)**

FA 14.2.0 Survivability ENGINEERING
CCA 14.2.3 Information Management
CCA 14.2.3.2 Information Maintenance

C1. Schedules identify when information/documentation is needed, and how often it must be updated which are consistent with the Integrated Master Schedule and contract requirements as well as with the information hierarchies. **(Q1, Q2, Q5, Q10))**
C2. Clear identification has been made as to who is responsible for developing information or documentation and who receives or is the ultimate user of the information. **(Q3, Q4, Q5)**
C3. Clear identification has been made in establishing the format and content requirements of the information/documentation. **(Q5)**
C4. There is a review process prior to information distribution for technical accuracy, sufficiency, and security classification. **(Q6)**
C5. Documents requiring government approval are identified and schedules accommodate government review/approve cycle. **(Q10)**
C6. There is a process for baselining documentation and controlling changes. **(Q7, Q8, Q10)**
C7. There is a process for formally archiving critical data. **(Q9)**

Q1. Have schedules been developed for information delivery which are consistent with the Integrated Master schedule and contract requirements? **(C1)**

Q2. Are the information delivery schedules compatible with established informational hierarchies? **(C1)**

Q3. Has an OPR (Office of Primary Responsibility) been identified for generating each informational need? **(C2)**

Q4. Have organizations required to provide assistance or contribute information to generation of a specific database or document been identified? Have they committed to this responsibility? **(C2)**

Q5. Have the users of this information been identified? **(C1, C2, C3)**

- Does the format and content of the information meet their needs?
- Does the schedule for delivery of information meet their needs?

Q6. Who is required to review the information prior to release? **(C4)**

- Who reviews/coordinates that the information is technically accurate?
- Who reviews/coordinates that the information is sufficient and complies with the users needs and all contract requirements?
- Who reviews the information for appropriate security classification and that the users of the data have the proper clearances and storage facilities?

Q7. What information requires configuration control and how is configuration control maintained? **(C6)**

- How are changes documented and controlled?
- How are changes to a specific database or document that may impact other databases or documents identified? How are these other databases and documents changed?

Q8. Is there a process for rapidly disseminating critical information or changes while still maintaining configuration control? **(C6)**

Q9. What information/data is archived, how, and where? **(C7)**

Q10. Does the document require government approval? **(C1, C5)**

- Do schedules allow sufficient time for the review/approve cycle?
- How are changes in response to government comments identified and controlled?

FA 14.2.0 Survivability ENGINEERING
CCA 14.2.4 Monitoring
CCA 14.2.4.1 Meetings

C1. Survivability provides timely program support and reduces overall program risk by actively participating in meetings to insure proper interpretation and application of survivability requirements and guidelines throughout the program. **(Q1, Q2, Q3, Q4, Q5, Q6, Q7, Q8, Q9, Q10, Q11, Q12)**
C2. Survivability has regular internal organizational meetings to insure uniform and consistent interpretation of requirements and guidelines by all survivability personnel, work issues, facilitate risk identification and mitigation, and reassess program priorities and needs. **(Q15)**
C3. Meetings are identified to insure the Government is adequately provided status of Survivability program. **(Q13)**
C4. Survivability actions or issues identified from meetings are documented and tracked to resolution. **(Q14)**

Q1. How is Survivability made aware of meetings which may require their support? **(C1)**

- Is there a weekly or monthly published meeting log of all projected program meetings and TIMs (Technical Interchange Meetings) where Survivability can determine whether their support would be useful?
- Is the program divided into Integrated Product Teams with a survivability representative on each team? Does the Survivability member attend all IPT meetings?

Q2. Does Survivability regularly meet with key design engineers? **(C1)**

Q3. Does Survivability attend design and design status reviews? Does Survivability participate in development of the meeting agendas? **(C1)**

Q4. Does Survivability regularly attend and participate in the Parts, Material and Processes Control Board (PMPCB)? Does Survivability participate in development of the PMPCB meeting agendas? **(C1)**

Q5. Does Survivability regularly attend and participate in Engineering Change Boards or Configuration Control Boards? **(C1)**

Q6. Does Survivability participate in Weight Control Boards and Power Management Boards? **(C1)**

Q7. Does Survivability participate in lnterface Control Working Groups? Does Survivability participate in development of the meeting agendas? **(C1)**

Q8. Does Survivability participate in Subcontractor and Vendor design and program status reviews? Does Survivability participate in development of the meeting agendas? **(C1)**

Q9. Does Survivability participate in Budget meetings? **(C1)**

Q10. Does Survivability participate in regular program status reviews to the Program Manager? **(C1)**

- Does Survivability participate in development of the meeting agendas?
- Does Survivability raise resource or interorganizational coordination problems for Program Management to address?
- Are issues and risks identified?

Q11. Does Survivability participate in System Engineering status reviews? Does Survivability participate in development of the meeting agendas? **(C1)**

Q12. Does Survivability participate in Test planning meetings, test readiness reviews, and post test reviews for testing that is survivability related? **(C1)**

Q13. What meetings with the Government does Survivability either give presentations or support? Are these adequate and sufficient enough in detail to provide the Government timely information regarding the survivability program? **(C3)**

- Are there regular Survivability TIMs with the Government? Do these TIMs include subcontractor participation?
- Does Survivability present survivability program status at Program Management Reviews with the Government? Does Survivability participate in discussions regarding other PMR presentations?

Q14. How are actions or issues raised in meetings tracked until resolution? **(C4)**

- Are there meeting minutes documenting the actions and issues?
- Are there dates and OPRs assigned to each action?
- In what meetings are action items and resolution of issues stateside?

Q15. Does Survivability regularly meet as an organization to discuss program status and issues? **(C2)**

- At these meetings are requirements and guidelines frequently reviewed to insure there are no misinterpretations or disagreements in interpretation by survivability personnel?
- Are manpower or coordination problems surfaced so that management action can be taken?
- Are program needs and priorities continually reassessed to insure optimum use of survivability resources or identify a requirement for additional resources?
- Are risks and issues surfaced so that appropriate actions can be taken?
- Are Lessons Learned discussed and applied?

FA 14.2.0 Survivability ENGINEERING
CCA 14.2.4 Monitoring
CCA 14.2.4.2 Data Review

C1. A process is established for reviewing data (test and analytical) for survivability impacts, accuracy, and adequacy. **(Q1, Q4, Q8, Q9, Q11, Q12)**
C2. Survivability reviews all analyses and test data used to demonstrate compliance or validate compliance with survivability requirements for accuracy, adequacy, and impacts. **(Q3, Q5, Q6, Q7, Q11)**
C3. Survivability reviews all manufacturing process, design, and specification change data for survivability impacts. **(Q10)**

Q1. What process is established which allows survivability to provide timely review of engineering data for survivability design impacts? **(C1)**

Q2. What databases should Survivability regularly review for adequacy, sufficiency, or program impact? **(C1)**

Q3. Has Survivability reviewed all data (test and analysis) used to demonstrate compliance with survivability requirements presented at major design reviews (SDR, PDR, CDR) for accuracy, adequacy, and impacts? **(C2)**

Q4. Has Survivability reviewed all survivability test anomalies or test failures for impact assessment and resolution? **(C1)**

Q5. Does Survivability review all hardness assurance data for accuracy and compliance with requirements? **(C2)**

Q6. Does survivability review all test plans, procedures, and test reports which are survivability related? **(C2)**

Q7. Has Survivability reviewed all data and documentation used to validate compliance to survivability requirements presented at subsystem and system FCA/PCAs? **(C2)**

Q8. Does Survivability review system operational anomalies or failures for survivability impact? **(C1)**

Q9. Does Survivability review all hardness maintenance and surveillance data for accuracy, adequacy, and impact? **(C1)**

Q10. Does Survivability review all proposed process, procedure, design, and specification changes for survivability impacts? **(C3)**

Q11. Does Survivability review historical data used from other programs for applicability and sufficiency? **(C1, C2)**

Q12. Are there special Technical Performance Measures (TPMs) for survivability that are being monitored? Are there TPMs which may have a survivability impact (e.g., weight, power) that should be monitored? **(C1)**

FA 14.3.0 Survivability OPERATIONS

CCA 14.3.1 Design

CCA 14.3.1.1 Survivability Design Application

C1. Survivability is addressed from the onset and integrated into the iterative design process. **(Q1, Q2, Q5, Q10, Q20, Q21)**
C2. There are adequate survivability databases and guidelines for design engineers to build survivability into design. **(Q6, Q7, Q11, Q12, Q13, Q14)**
C3. Trade studies are performed to optimize survivability design with other performance requirements versus cost, schedule, and technical risk. **(Q3, Q4)**
C4. Factors such as uncertainties in survivability design verification, required production controls, and complexity/cost of system survivability maintenance throughout the operational life are considered during the design process. **(Q8, Q9, Q10, Q11, Q15, Q16, Q17, Q18, Q19, Q20, Q21)**
C5. Survivability design is verifiable and incorporates features which allow the system to withstand and meet all functional performance requirements trans and post threat attack throughout its specified life. **(Q11, Q15)**

Q1. How is survivability integrated into the design process? **(C1)**

- How has survivability been addressed in overall system architecture and design approach?
- Has allocation of survivability requirements been continually reassessed as design is iterated and optimized?
- Have survivability design drivers been identified?
- Has survivability been factored into design risk assessments?

Q2. Is design accomplished through Integrated Product Teams with a survivability specialist as an IPT member? If not, how is survivability support provided to design engineering? **(C1)**

Q3. What trade studies have been identified for meeting system survivability requirements? **(C3)**

- Proliferation vs. Hardening
- Ground Terminal vs. On-Board Satellite processing
- Communication frequency and modulation
- Passive vs. Active Defense
- Mobility or Maneuver vs. level of hardening
- Level of Command and Control Segment survivability vs. Space Segment autonomy
- Satellite to satellite crosslinks vs. dispersed Ground Nodes

Q4. What trade studies have been identified for meeting single satellite or ground terminal survivability requirements? **(C3)**
For example,

- What radiation shielding topologies have been considered? For example, spacecraft level vs. box level vs. component level or some combination of each.
- What HEMP shielding topologies have been considered? For example, shielded enclosure vs. cable/box or some combination of each.

- What hardware vs. software trades have been performed? For example, use of SEU immune components as opposed to implementation of software error detection and correction
- Level of component and circuit hardening as opposed to implementation of a circumvention and recovery.
- Level of hardening vs. availability of redundant subsystems
- Optics hardening vs. shutters
- Hardening approach vs. cost/complexity of hardness maintenance/hardness surveillance

Q5. Have survivability requirements been allocated down to the piecepart level? **(C1)**

Q6. Has survivability provided design engineers Survivability Design Guidelines and databases to assist them in implementing survivability into design? **(C2)**

- Are X-ray and total dose radiation shielding effectiveness profiles provided for a variety of shielding materials?
- Are piece part radiation derating factors and end-of-life data provided for total dose and neutron displacement damage?
- Are SEU rate piecepart data provided?
- Are SEL susceptible pieceparts identified?
- Are TREE upset levels provided for components?
- Are there guidelines and data for how to implement current limiting into circuit design to prevent photocurrent burnout?
- Are there guidelines for implementing photocurrent compensation?
- Are design guidelines provided for preventing latchup?
- Are there guidelines for how to implement spike adaptive threshold techniques?
- Are there databases for component photocurrent burnout and SGEMP burnout levels?
- Is there SGEMP data on a variety of cable types?
- Are there guidelines for selecting terminal protection devices?
- Are there guidelines for use of low Z coatings that can be used to mitigate against box IEMP?
- Are grounding guidelines provided to assist the designer in mitigating against ECEMP?
- Are there guidelines and databases provided to develop a design resilient to damage from thermomechanical shock?
- Are guidelines given for what materials are approved (or disapproved) for certain applications because of radiation and/or laser response characteristics?
- Are guidelines and databases provided to remove susceptibilities to laser induced red out in optics?
- Are guidelines given for epoxying of components, staking or tie down?
- Are guidelines established for minimum acceptable design margins for each threat environment or effect?
- Are guidelines and databases provided for identifying the appropriate application of and designing circumvention/recovery circuitry?
- Are guidelines provided on RF shielding and penetration designs to prevent leakage or backdoor coupling?

- Are databases provided to assist in designing against Jammer or HPM front end burnout?

Q7. Has Survivability reviewed the approved parts list (APL) and component data sheets? **(C2)**

Q8. Has Survivability established piecepart qualification and lot acceptance test levels and samples sizes? **(C4)**

Q9. Has Survivability established guidelines where parts must be 100% screened in a particular environment? **(C4)**
For example,

- Are devices which are not latchup immune 100% latchup screened for use in certain applications?

Q10. Are design margin allocations at various levels of integration consistent with: **(C1, C4)**

- Piecepart test program?
- Test uncertainties?
- Analytical uncertainties?

Q11. Has Survivability identified what analyses are required to be performed in order to verify design compliance with requirements? **(C2, C4, C5)**

- Has Survivability defined the approved methodology for performing these analyses?
- Have these analyses been presented to the Government at the appropriate design reviews?

Q12. Has Survivability provided subcontractors and vendors necessary databases and design guidelines for incorporating survivability into their design? **(C2)**

- Has survivability provided subcontractors and vendors an approved methodology for demonstrating requirement compliance?

Q13. Has Survivability performed ray trace analyses at varying levels of integration to insure there are no unexpected shadowing or illumination paths? **(C2)**

Q14. Has Survivability identified characterization tests and engineering tests to support design development and analytical model verification? **(C2)**

Q15. Is there are credible survivability validation program which incorporates analysis and test and demonstrates required system functional performance trans and post attack? **(C4, C5)**

- What is the method of validating design compliance at each level of integration for each specified threat?
- Is the method of validation appropriate considering design risk or uncertainty? Are there margins in test levels or threat environments used in analyses over the predicted threat levels?

Q16. Have hardness critical items and hardness critical processes been identified on design drawings? **(C4)**

Q17. Is software documentation annotated to identify survivability and special security functions? **(C4)**

Q18. Have all special handling and assembly or tolerance requirements been identified and incorporated in the proper production documentation? **(C4)**

Q19. Besides piecepart hardness assurance testing during production, are there any circuit level (e.g., circumvention circuitry), box, or higher level of integration acceptance tests required to insure survivability capabilities are maintained during production? **(C4)**

Q20. Has hardness maintenance and surveillance of the system been factored into the design process? **(C1, C4)**

- What production data is required to support performance baselines for hardness maintenance and surveillance.
- Are there any shelf life sensitive components?
- What spare parts inventories are required to maintain the system over its lifecycle?
- What special test equipment is needed for hardness surveillance?
- What special training is required to implement a hardness maintenance/surveillance program?
- Have special storage and transport requirements been identified? For example, do components require constant Nitrogen purge?

Q21. Has the design process identified unique satellite storage requirements? **(C1, C4)**

- For example, do components require constant Nitrogen purge?
- Are there any shelf life sensitive components that must regularly be replace or replace just prior to launch?
- What spare parts inventory should be maintained?
- Are there periodic tests required during storage to insure maintenance of survivability capabilities?

FA 14.3.0 Survivability OPERATIONS
CCA 14.3.1 Design
CCA 14.3.1.2 Survivability improvement or changes

C1. There is a process for identifying areas for survivability improvements based on availability of new technology. **(Q1)**
C2. There is a process for identifying necessary survivability design changes because of parts obsolescence. **(Q2)**
C3. There is a process for identifying manufacturing process changes which enhance survivability and for assessing survivability impacts of other proposed manufacturing process changes. **(Q3, Q4)**
C4. There is a process for identifying design susceptibilities and potential vulnerabilities and proposing survivability improvements. **(Q5, Q6)**
C5. There is a mechanism for testing, and evaluating proposed survivability improvements prior to decisions to implement. **(Q7)**
C6. Full lifecycle impacts on operations, documentation, plans, and procedures have been identified and revisions made accordingly. **(Q8, Q9)**

Q1. Is technology state of the art being monitored? Have new technologies (hardware and software) become available which can enhance survivability performance? **(C1)**

Q2. Have vendors gone out of business or are parts no longer being made which impact production or maintenance of adequate spares over the system lifecycle? **(C2)**

- Have survivability impacts been assessed?

Q3. Are there manufacturing process changes which can enhance survivability performance or improve design margin? **(C3)**

- Are they changes to the Hardness Assurance and acceptance test program?
- Are they changes to assembly and handling procedures?
- Are they changes to material coating processes?

Q4. Are all proposed manufacturing changes assessed for survivability impact? **(C3)**

Q5. Have any design specific threat susceptibilities (hardware and software) been identified which can be potentially (and realistically) exploited or are within the realm of uncertainty in threat definition? **(C4)**

- Are there changes to the design which can eliminate these susceptibilities or make the design immune to slight variations in a threat scenario parameter?

Q6. Has DIA identified new threats which are outside of or exceed the threat envelope specified in the system design specifications and design requirements documents? **(C4)**

- Are there test and analytical data which have identified a vulnerability to this threat?
- Can modifications be made to the design to mitigate against the new threat?

Q7. What tests and/or analyses need to be performed to verify the proposed survivability design change provides the expected capability? **(C5)**

Q8. What other documentation, plans, and procedures must be revised to accommodate this change? **(C6)**

Q9. Does implementation of the change require new special test equipment or new training procedures? **(C6)**

FA 14.3.0 Survivability OPERATIONS
CCA 14.3.1 Design
CCA 14.3.1.3 Deficiency Correction Design

C1. There is a mechanism for formally documenting survivability design deficiencies identified through analyses, data reviews, testing, or operations and implementation of corrective actions. **(Q1, Q6, Q7, Q13)**
C2. There is a mechanism for assessing survivability design impacts based on alerts issued from other programs and taking corrective actions as appropriate. **(Q2, Q3)**
C3. There is a mechanism for formally investigating test anomalies and failures, documenting the cause of the anomaly or failure, and the associated corrective actions. **(Q4, Q5, Q8)**
C4. There is a mechanism for formally documenting survivability deficiencies identified in Independent Operational Test and Evaluation and, if applicable, Live Fire Tests and implementing the necessary corrective actions. **(Q9, Q10, Q11, Q12)**

Q1. Once a design is baselined and placed under configuration control, how are survivability design deficiencies or potential deficiencies which are identified through further analyses, data reviews, or testing formally documented and tracked until corrective actions are implemented? **(C1)**

- Does this mechanism for identifying deficiencies and tracking resolution include both hardware and software problems?
- What documentation identifies the deficiency or potential deficiency? Does it identify a strategy for resolution and estimated schedule?
- If further study is required is this annotated on the document? Are manpower and other necessary resources noted?
- Who coordinates on and who gives final approval on the strategy for closure?
- Who coordinates on and who gives final approval that the appropriate corrective action has been implemented?
- Are Engineering Change Notices issued prior to drawing changes associated with any corrective action? Are these ECNs approved through the Configuration Control Board?

Q2. How are GIDEP alerts monitored and program impacts assessed and documented? **(C2)**

- Are GIDEP alerts tracked through the PMPCB or other organization?
- How are program impact assessments formally documented? Is the manner of documentation dependent on whether the assessment concludes there is a design deficiency or not?

Q3. Is there a mechanism for assessing program impact due to failures or anomalies experienced on other programs? How are these issues formally tracked and documented? **(C2)**

Q4. Is there a mechanism for identifying, formally tracking, and documenting test failures and associated corrective actions? **(C3)**

- Are all component, subsystem, and system test failures or anomalies which occur during formal qualification testing, acceptance testing, or other major tests formally documented in a Failure Analysis Report (FAR) or other document?
- Is there a formal mechanism (who gets contacted and how) and are timelines established for notifying the Government of the failure?
- Are the test conditions of the failure and the observed effects fully documented?
- Are there regular updates on the status of the Failure Investigation?

- Is all data documented which support the failure investigation team's findings regarding what caused the failure?
- Are corrective actions documented including identification of associated drawing revisions and procedural changes?

Q5. Is there a Failure Review Board (FRB) which is responsible for providing the manpower and special expertise to support failure investigations, review and approve the investigation findings and recommendations? **(C3)**

- Who are the members of and who chairs the FRB?
- What is Survivability's role with respect to the FRB?

Q6. Are corrective actions fully tested and/or analyzed prior to implementation? **(C1)**

Q7. How is configuration control maintained in implementing a change? (C1)

Q8. If a deficiency is uncovered during a specific qualification test performed in a test series are the impacts of the failure and required corrective action on the validity of prior qualification tests which were successfully passed assessed? **(C3)**

Q9. What is the mechanism for formally documenting survivability deficiencies identified during Live Fire Tests if the program is required per DoD 5000.2 to perform this test? **(C4)**

- Who should participate on the failure investigation team?
- Is all data documented which support the failure investigation team's findings regarding what caused the failure?

Q10. What is the process for developing design fixes for deficiencies identified during Live Fire Tests? **(C4)**

- Are proposed fixes fully tested and analyzed prior to implementation?
- How is configuration control maintained?

Q11. What is the mechanism for formally documenting survivability deficiencies identified during Independent Operational Test and Evaluation (IOT&E)? **(C4)**

Q12. What is the process for evaluating these deficiencies identified during IOT&E and developing fixes as appropriate? **(C4)**

- Are causes for the deficiencies fully identified?
- Have proposed fixes been fully tested and analyzed before being implemented?
- How is configuration control maintained during change implementation?

Q13. What is the mechanism for formally documenting survivability deficiencies or anomalies which may indicate potential survivability anomalies during system operation? **(C1)**

- What is the process for having deficiencies or anomalies evaluated for impact?
- What is the process for taking corrective action?
- How is the impact to system operation minimized?

FA 14.3.0 Survivability OPERATIONS
CCA 14.3.2 Testing
CCA 14.3.2.1 Qualification Testing

C1. A comprehensive qualification test program is a key element of system survivability design verification. **(Q1, Q2, Q6)**
C2. There is a clear interrelationship between analyses and qualification tests used to verify compliance with overall system survivability requirements including use of test data to help validate system analytical models. **(Q2, Q3, Q6)**
C3. Qualification tests should be performed at multiple levels of integration and up through the highest level of integration practical. **(Q5, Q7, Q8, Q9, Q10)**
C5. Qualification test schedules should be realistic. **(Q4, Q11, Q12, Q13, Q14)**
C6. Sufficient resources have been allocated to support pre-test planning, qualification testing and potential troubleshooting, and post test evaluation. **(Q11, Q12, Q15, Q16)**
C7. Qualification test requirements establish the basis for the hardness assurance test program and production acceptance test requirements. **(Q17, Q18)**

Q1. Are qualification tests identified in the system survivability qualification plan or other program document? **(C1)**

Q2. Is there a solid technical rationale for supporting the mixture of analyses and tests used to verify compliance with system survivability requirements? **(C1, C2)**

Q3. How do characterization testing and engineering tests support qualification test planning? **(C2)**

Q4. Do qualification test plans and procedures require Government approval? If so, has the timing for submittal of these documents allowed sufficient time for review and comment? **(C5)**

Q5. For the particular threat environment, is testing performed at the appropriate levels of integration including the associated flight or operational software? **(C3)**

- Are pieceparts qualification tested?
- Are special circuits or circuit cards qualification tested?
- Are boxes qualification tested?
- Are subsystems qualification tested?
- Are configuration items qualification tested?
- Are there segment level qualification tests?
- Are there system level qualification tests?

Q6. How are special survivability/security functions tested during software formal qualification testing (FQT)? **(C1, C2)**

Q7. Is testing being performed at the highest level of integration practical to reduce the risk of missing hard to predict failure mechanisms such as: **(C3)**

- sneak paths
- design response synergies
- hardware/software incompatibilities?

Q8. What is the piecepart radiation qualification test program? **(C3)**

- How are test levels and pass/fail criteria established?
- Have appropriate design margins been factored into the qualification test levels?
- What are the total dose test requirements?
- What are the neutron irradiation test requirements?
- What are the prompt dose and dose rate test requirements?
- What are the pulse overstress test requirements?

Q9. Does the box and subsystem qualification test program include such things as: **(C3)**

- Flash X-ray (FXR) electronic box and subsystem tests?
- Current injection testing (CIT) of electronic boxes?
- Free field electromagnetic illumination tests of boxes and subsystems?
- Box level vibration testing?
- Pulsed laser and RF testing?
- Optical performance response testing?
- Simulation of signal processor response to sensor focal plane radiation hits?

Q10. What segment and system testing is planned? **(C3)**
For example,

- Are there anti-jamming communication and data link qualification tests?
- Are there anti-scintillation communication and data link performance tests?
- Are there low probability of intercept tests?
- Are there user terminal EMP field illumination tests?
- Are there user terminal blast and shock tests?
- Are there system autonomy tests?
- Are there system software security tests?
- Are there system computer security tests?
- Are there system physical security tests?
- Are there system communications security tests?

Q11. Is special test equipment necessary to support qualification testing? **(C5, C6)**

- Have test hardware and test software requirements been identified?
- Is the schedule for development or purchase of STE compatible with the Qualification test schedule?
- Is the schedule for training personnel to operate STE compatible with the Qualification test schedule?

Q12. Are special test facilities required? **(C5, C6)**
If so, have

- facilities been scheduled and funding arranged?
- Unique facility requirements or limitations/conditions been identified?

Q13. Are the qualification test schedules realistic and based on historical performance? **(C5)**

- Does the test sequence make sense?
- Is there time incorporated in the test schedules for reconfiguration of the article if required between tests?
- Is there sufficient time built into the schedule to allow for some facility problems?

- Is there sufficient time built into the schedule to troubleshoot minor anomalies?

Q14. Have contingencies been planned in the event a test must slip or a test runs longer than planned? **(C5)**

- What arrangements have been made with other programs who may be scheduled to use the test facilities?

Q15. Have sufficient resources been identified to support qualification testing? **(C6)**

- What are the manpower requirements from the Test, Survivability, and Design organizations?
- Are there manpower and resources to support pre-test planning, test execution, and post test analysis?
- Is there manpower available to support troubleshooting of test equipment and test software if required?
- Is there manpower available to support troubleshooting of system hardware and software if required?

Q16. How are survivability qualification test data and performance evaluations documented? **(C6)**

- Are there contract deliverable test reports?
- Who writes the survivability qualification test reports?
- Who provides the survivability post test performance evaluation?

Q17. What is the relationship between qualification test requirements and hardness assurance/acceptance test requirements? **(C7)**

Q18. Are qualification test results used to reassess the adequacy of the hardness assurance and production acceptance test requirements? **(C7)**

FA 14.3.0 Survivability OPERATIONS
CCA 14.3.2 Testing
CCA 14.3.2.2 Production Testing

C1. Production testing and controls are implemented which assure the as-designed survivability is maintained throughout system manufacture, assembly, and build. **(Q1, Q2, Q3, Q4, Q5, Q6, Q7)**
C2. Production schedules include realistic times for production testing. (**Q10)**
C3. Sufficient resources are available to support production testing. **(Q8, Q9)**
C4. Production data assist in establishing a performance baseline for hardness maintenance and surveillance of the delivered system. **(Q6, Q11, Q12)**

Q1. Is there a Hardness Assurance Plan? Does it identify specific tests and controls for production to insure survivability capabilities of the designed system are maintained throughout production? **(C1)**

Q2. What production piecepart lot acceptance tests and 100% screens are required? For example, What are the sample sizes, test requirements, and pass/fail criteria for radiation lot acceptance? **(C1)**

- What parts require 100% screening for latchup?
- Is pulse overstress testing required on any components?

Q3. Are there tests identified for any components or circuits that must have special calibration or response data taken? **C1)**

- Are there circuits that require "matched" components (for selection of a resistor value for thresholding in a circumvention circuit or circuits which require matched filters?
- Is calibration data required for use in system software data tables?

Q4. Are there any production tests that have to be performed on every delivered unit because the design failed to meet large enough design margins during qualification testing? **(C1)**

- What are these tests, what are the test levels, and what are the pass/fail criteria.

Q5. Are there production process controls to ensure that survivability is maintained through process and assembly? **(C1)**
For example,

- Are there special inspection requirements of shielding materials for scratches?
- Are there contamination controls on sensitive devices? How are these verified--inspection or test?
- Are there special survivability related actions identified in assembly procedures?

Q6. Are hardness critical items and processes identified on drawings? **(C1, C4)**

Q7. Is there provision for motivation and awareness training that acquaint production personnel with hardness/survivability critical procedures and processes? **(C1)**

Q8. What special test equipment is required for the performance of production testing and to support potential troubleshooting? **(C3)**

Q9. Have sufficient resources been identified to support production testing? **(C3)**

- What are the manpower requirements in Test, Survivability, QA, and Design?
- Is there manpower available to support troubleshooting of test equipment and test software if required?
- Is there manpower available to support troubleshooting of system hardware and software if required?

Q10. Are schedules for production acceptance testing realistic? **(C2)**

- Do they account for potential conflicts in use of test facilities or test equipment?
- Do they allow for possible test equipment problems?
- Do they allow for possible troubleshooting of hardware and software?
-

Q11. What production data are required to support the hardness maintenance and surveillance program? **(C4)**

- Where are these data needs documented?
- How are the data archived-- in contract deliverable test reports?

Q12. Is there a Hardness Maintenance and Surveillance Program Plan containing a complete description of survivability maintenance activities for the fielded system including surveillance tests and evaluation activities? **(C4)**

FA 14.3.0 Survivability OPERATIONS
CCA 14.3.2 Testing
CCA 14.3.2.3 Survivability Improvement Testing

C1. There is a survivability characterization and engineering test program to support design evolution. (**Q1, Q2, Q3, Q4)**
C2. There is a survivability test program to support susceptibility and vulnerability analyses in identifying areas for potential survivability improvements. **(Q5)**
C3. There is a test program to support feasibility of proposed improvements. **(Q6, Q7, Q8)**

Q1. Is there a survivability characterization test program to provide the necessary databases to support design? **(C1)**
For example,

- What component or material radiation tests are planned?
- What material laser response tests are planned?
- Are there tests to characterize particular cable designs for SGEMP response?
- What pulse overstress tests are planned?

Q2. Where are characterization test requirements documented and where is data archived? **(C1)**

Q3. What engineering tests are planned to evaluate the performance of critical or sensitive circuits? **(C1)**

Q4. What engineering tests are planned to evaluate software/hardware interactions where interfaces are complex and timing critical? **(C1)**

Q5. What tests are being performed to support susceptibility and vulnerability analyses? **(C2)**

- Is characterization testing carried through to levels where upset occurs?
- Is characterization testing carried through to levels where damage occurs?
- Is performance degradation as a function of increased test levels being characterized for certain environments?
- Is there a test program to establish fragility curves as a function of peak threat exposure level and duration?

Q6. What testing is required to support verification of a proposed survivability improvement prior to implementation? **(C3)**

Q7. How does implementation of the survivability improvement impact qualification of the system design? **(C3)**

Q8. Besides development testing, will there be operational tests to verify the action provides a survivability improvement? **(C3)**

FA 14.3.0 Survivability OPERATIONS
CCA 14.3.2 Testing
CCA 14.3.2.4 Analytical Fidelity Improvement

C1. Testing is used to reduce uncertainties in survivability analytical predictions and to flush out the "unknown unknowns". **(Q1, Q2, Q4, Q5, Q6, Q7, Q8, Q9)**
C2. Testing is used to support calibration and validation of system survivability models. **(Q3, Q4, Q5, Q6, Q8, Q9)**

Q1. What test data are required to reduce known uncertainties in analytical models and predictions? **(C1)**

- What level of system integration or level of assembly is required to undergo test to address these uncertainties?

Q2. What tests are being performed to address "unknown unknowns" in analytical predictions? **(C1)**
For example,

- What tests are designed to flush out sneak paths or unknown coupling paths?
- What tests are designed to flush out synergistic responses?
- What tests are designed to flush out hardware/software incompatibilities?
- Are tests being performed at the appropriate level of integration to identify these effects?

Q3. What tests and test data are required to support calibration and validation of system models? **(C2)**

Q4. What uncertainties are introduced because of uncertainties in the test environment or limitations in test environment fidelity to the threat environment? **(C1, C2)**

Q5. When are the tests to obtain this data scheduled? Are the test schedules compatible with schedules for when the analyses are needed? **(C1, C2)**

Q6. Are tests to obtain the necessary data incorporated into an already planned test series such as characterization test series or qualification test series? **(C1, C2)**

- If so, do the test plans need to be modified to obtain the data needed?

Q7. Have subcontractors identified a test program to reduce uncertainties in their analytical models and predictions and flush out unknowns? **(C1)**

Q8. How are test results documented? **(C1, C2)**

Q9. Are changes in design evaluated for impact on validity of this test data for supporting analytical model improvements or validation? **(C1, C2)**

FA 14.3.0 Survivability OPERATIONS
CCA 14.3.2 Testing
CCA 14.3.2.5 Corrective Action Verification

C1. There are test data to support design fixes in response to identified design deficiencies will comply with all survivability requirements. **(Q1, Q2, Q3, Q4)**
C2. There are test data to ensure design fix was implemented correctly. **(Q5)**
C3. All impacts of corrective action implementation on test have been identified. **(Q5, Q6)**

Q1. Are test data required to verify that there is a design deficiency and to identify the cause of the deficiency? **(C1)**

Q2. What test data are required to support development of alternative fixes for a design deficiency? **(C1)**

Q3. What test data are required to evaluate the adequacy of a proposed fix for a design deficiency in meeting survivability requirements? **(C1)**

Q4. What test data are required to ensure the proposed fix does not cause problems in other areas of the design in meeting survivability requirements? **(C1)**

Q5. What test data are required to verify the implemented fix meets requirements? **(C2, C3)**

- Will the design have to undergo a full or partial requalification?

Q6. Does the fix impact what is required for production acceptance testing, acceptance test levels, and pass/fail criteria? **(C3)**

FA 14.3.0 Survivability OPERATIONS
CCA 14.3.3 Feedback Reporting
CCA 14.3.3.1 Reporting System Development

C1. Ensure survivability is incorporated into a program's system for identifying and reporting anomalies, failures, and incidents which complies with government requirements through all program phases. **(Q1, Q2, Q3, Q4, Q5, Q6, Q7)**
C2. Ensure there is a feedback reporting process for evaluating the efficacy of process or procedural changes implemented on the program which affect survivability. **(Q9)**
C3. Reporting system establishes guidelines for the maximum time allowed between the occurrence of an anomaly/failure/incident and notification. **(Q8)**
C4. Reporting system establishes guidelines for problem evaluation, impact assessment, resolution, and closure. **(Q10, Q12)**
C5. Reporting system allows problems to be tracked and appropriate resources applied to reach resolution and closure. **(Q11)**
C6. Reporting system archives problems and anomalies to allow survivability-related trend patterns to be established and support investigations of future anomalies and failures. **(Q13, Q14)**

Q1. What is the process for reporting anomalies, failures, and incidents during design development for both hardware and software and how are impacts assessed for survivability impacts? **(C1)**

Q2. What is the process for reporting anomalies, failures, and incidents during production and how are impacts assessed for survivability impacts? **(C1)**

Q3. What is the process for reporting anomalies, failures, and incidents during storage and how are impacts assessed for survivability impacts? **(C1)**

Q4. What is the process for reporting anomalies, failures, and incidents during transportation and deployment and how are impacts assessed for survivability impacts? **(C1)**

Q5. What is the process for reporting anomalies, failures, and incidents during system operations and how are impacts assessed for survivability impacts? **(C1)**

Q6. What is the process for reporting anomalies, failures, and incidents during system maintenance and how are impacts assessed for survivability impacts? **(C1)**

Q7. What is the process for reporting anomalies, failures, and incidents during system decommissioning/disposal? **(C1)**

Q8. What are the guidelines for maximum time allowed for reporting anomalies, failures, and incidents and do these comply with government requirements? **(C3)**

- Do the guidelines identify specifically who should be notified and how?

Q9. Is there a feedback reporting process established for evaluating the efficacy of process or procedural changes? **(C2)**

- Does the process identify who provides the feedback data and who evaluates it?
- Does the process identify how often reports are provided?

- Does the information collected allow survivability technical assistance to be more effective and more timely?
- Does the information collected allow survivability impact assessments to be more effective and more timely?

Q10. What are the guidelines for what information should be documented in anomaly, failure, and incident reports and do these comply with government requirements? **(C4)**

- Do reports document what system level of assembly was involved (including appropriate serial numbers), when, where, and under what conditions (ambient, thermal vacuum, etc.) an anomaly, failure, or incident occurred?
- Do reports provide a description of the failure?
- Do reports identify likely cause(s) and provide data to support conclusions?
- Do reports identify whether problem is generic or an isolated case and provide supporting data for the position?
- Do reports document minority positions?
- Do reports identify proposed corrective action and items affected (hardware, software, drawings, and documentation).

Q11. How does management track anomaly, failure, and incident reports and insure proper resources are applied to reach resolution? **(C5)**

Q12. Who coordinates and who provides signatures for final closeout of an anomaly, failure, or incident reports? **(C4)**

Q13. Who is responsible for archiving anomaly, failure, and incident reports? **(C6)**

Q14. Does survivability maintain trend data on anomalies, failures, and incidents which may have impacts on system survivability capabilities? **(C6)**

- How is trend data archived?

FA 14.3.0 Survivability OPERATIONS
CCA 14.3.3 Feedback Reporting
CCA 14.3.3.2 Report Accounting

C1. Failure, anomaly, and incident reports are statussed and updated frequently enough and at a high enough level of management to permit realistic survivability impact assessments and preparation of mitigation actions. **(Q1, Q2, Q3, Q4)**
C2. Reports are archived to permit trend monitoring for potential survivability impacts and to assist in evaluation of other failures, anomalies, and incidents. **(Q5, Q6)**
C3. Report closure requires management sign-off and coordination across sufficiently broad technical disciplines including survivability. **(Q7)**
C4. Reports comply with all government requirements for format, content, frequency of submittal, and distribution. **(Q8, Q9)**

Q1. How does management track failure, anomaly, and incident reports? **(C1)**

Q2. Are status updates provided frequently enough to allow realistic program impact assessments to be made so that effective mitigating actions can be taken? **(C1)**

Q3. Are failures, anomalies, and incidents which impact the survivability of the system identified? **(C1)**

- Does survivability provide program impact assessments?

Q4. How is the Government kept informed of failure, anomaly, and incident program impacts and status of associated investigation and follow-up actions? **(C1)**

Q5. Who is responsible for and where are archives of failure, anomaly, and incident reports maintained? **(C2)**

Q6. How are archives maintained throughout the life of the system? **(C2)**

Q7. Have proper signatures been obtained for report closure? **(C3)**

- Does closure require sign-off by the program manager?
- Does closure require sign-off by the system engineer?
- How does survivability coordinate on report closure?

Q8. Do reports comply with all contract requirements including format, content, frequency of submittal, and distribution? **(C4)**

Q9. For operational systems, do reports comply with operating agency guidelines or procedures? **(C4)**

FA 14.3.0 Survivability OPERATIONS
CCA 14.3.4 Corrective Actions
CCA 14.3.4.1 Accounting System Development

C1. Ensure there is a process for documenting design changes to correct design deficiencies which involves Survivability. **(Q1, Q2, Q3, Q4)**
C2. Ensure impacts of implementation of corrective action on survivability are fully identified. **(Q2)**
C3. Ensure that configuration control of the system is maintained during the process of implementing corrective actions. **(Q5, Q6)**
C4. Ensuring all affected program documentation is changed to reflect the corrective action taken. **(Q7)**
C5. System meets all government contract requirements. **(Q8)**

Q1. What documentation is required to support a design change to correct a design deficiency? **(C1)**

- What survivability analyses and test data are required?

Q2. What documentation is required and what is the approval process for implementing a design change? **(C1, C2)**

- Who must coordinate or signoff on these documents?
- Is the reason for the change identified?
- How does survivability coordinate on design changes prior to their implementation?

Q3. Do Engineering Change Notices (ECNs) require rationale for the change and identify all documents affected? **(C1)**

Q4. How are ECNs categorized to indicate whether Government approval is required or not? **(C1)**

- Does classification depend on whether contract cost or contract schedule is impacted, and whether it impacts form, fit, or function of the system as defined by government approved specifications?
- Does the DCMC (DCAS/DPRO) review all ECNs for proper classification and technical accuracy for the government per Memorandum of Agreement?

Q5. How is configuration control maintained during the change process? How does survivability know they are assessing the correct design? **(C3)**

Q6. Is there a Configuration Change Board (CCB) which reviews and approves proposed changes, evaluates the adequacy and accuracy of the supporting data and documentation, concurs with classification of the change and program impact? **(C3)**

- Who are the members and who chairs the CCB?
- What is Survivability’s role with respect to the CCB?

Q7. What process is implemented to ensure all affected documentation is changed or updated? How does survivability support this process? **(C4)**

- Specifications?
- Databases?

- Drawings? Do changes to hardness critical items and processes need to be made?
- Survivability Design Guidelines
- Assembly Instructions
- Inspection procedures
- Test plans, procedures
- Survivability Analyses
- Hardness Assurance program documentation
- Hardness Maintenance and Surveillance program documentation

Q8. Does the corrective action accounting system comply with all government requirements? **(C5)**

- Does it meet all configuration management requirements?
- Does it comply with contract in identifying actions which require government approval?
- Does it comply with cost and schedule reporting requirements?

FA 14.3.0 Survivability OPERATIONS
CCA 14.3.4 Corrective Actions
CCA 14.3.4.2 Corrective Actions Accounting

C1. There is a process for tracking changes to correct deficiencies and maintaining configuration control to ensure survivability of the system is attained or maintained. **(Q1, Q2, Q3)**
C2. All corrective actions have been assessed for survivability impact including risk. **(Q4, Q5, Q6)**

Q1. Are actions required to correct specific survivability deficiencies identified and tracked as survivability issues? **(C1)**

Q2. How is survivability made aware of design or production changes required to correct non-survivability related deficiencies to verify the changes will not degrade system survivability? **(C1)**

Q3. How are changes identified and how is configuration control maintained? **(C1)**

- How are specification changes identified?
- How are survivability database and survivability guideline document changes identified?
- How are drawing changes identified?
- How are assembly instructions and inspection procedure changes identified?
- How are revised survivability test plans/procedures identified?
- How are revised hardness maintenance/surveillance procedures identified?

Q4. How does survivability review changes to documentation for survivability impact and document their findings? **(C2)**

- Which documents require survivability sign-off?
- How is survivability coordination accomplished in cases where survivability does not specifically sign off on a document?

Q5. How is validation data (test and analyses) documented and maintained which supports the corrective action either had no impact on survivability capabilities, corrected a survivability deficiency, or provided a survivability improvement? **(C2)**

Q6. How does survivability identify and document a change in overall survivability risk associated with a specific corrective action? **(C2)**

Appendix A. Glossary of Survivability Terms

Avoidance	Incorporation of measures that make a system difficult to detect, attack, or hit. Avoidance measures may include stealth or tactics.
Active Defense	The use of measures (such as a missile defense system or electromagnetic countermeasures) to enhance a system's survivability by destroying incoming weapons or causing them to detonate outside of the susceptible area of the protected system.
Blackbody Spectrum	Spectrum of photon energies emitted from a body in thermodynamic equilibrium. Nuclear weapons produce hot plasmas (~10^7 K) which are nearly in thermodynamic equilibrium from which most of the total energy released by the weapon is radiated as thermal energy with black body spectra with photon energies in the X-ray region.
Blackout	Loss of a communications link due to severe absorption as signal is propagated through the nuclear environment or highly disturbed ionosphere.
Blast Loading	The loading or force on an object caused by the air blast from an explosion striking and flowing around the object. It is a combination of overpressure (or diffraction) and dynamic pressure (or drag) loading.
Blast scaling laws	Formulas which permit the calculation of the properties, e.g., overpressure, dynamic pressure, time of arrival, duration, etc., of a blast wave at any distance from an explosion of a specified energy from the known variation with distance of these properties for a reference explosion of known energy.
Blowoff Impulse	Impulse delivered to a surface when material is removed by vaporization, melt, and/or spallation usually due to the absorption of cold X-rays.
Bremsstrahlung	Radiation in the X-ray region due to interaction of high energy electrons with matter.
Circumvention and Recovery	Processes including: detection of the leading edge of oncoming prompt radiation, activation of protective modes/devices (typically powering off), and reconstitution of the system after the radiation pulse has subsided.
CIT	Current Injection Testing. Method for simulating SGEMP induced currents.
Cobalt 60 source	A gamma ray source used to simulate the total dose produced by a nuclear weapon or the dose received from the natural radiation belts.
Cold X-rays	The lower energy (~ 1-10 keV) X-rays from a nuclear burst.
Curling	Permanent deformation of structures due to plastic compressive yielding near surfaces exposed to cold X-rays.
Debris Gamma	The delayed gamma rays that come from the radioactive fission products and various neutron capture reactions produced by a nuclear weapon..
Deception	The use of measures to deceive the enemy as to actual system location thereby drawing fire away from the target.
DIA	Defense Intelligence Agency
Direct Ascent ASAT	Refers to a nuclear or conventional Anti-Satellite (ASAT) attack launched from the ground against one or more satellites.
Displacement Damage	Displacement of atoms in a crystal lattice usually by neutrons leading to degradation of transistor gain or increases in bulk resistivity.
Dose Rate	The peak ionizing dose rate (energy/unit mass/unit time) produced by a nuclear weapon
ECEMP	Electron Coupled Electromagnetic Pulse results from penetrating electrons which buidl up a coulombic charge on ungrounded accumulators.
EMP	The Electromagnetic Pulse of RF radiation produced when an explosion occurs in an unsymmetrical environment, especially at or near the earth's surface or at high altitudes. In Nuclear EMP, X-rays and Gamma rays from a nuclear weapon generate Compton electron currents in the atmosphere and ground.

Enhanced Belts	Increased electron and proton fluxes in the trapped radiation belts due to the exoatmospheric detonation of one or more nuclear weapons.
Fallout	Particles contaminated with radioactive material from the radioactive cloud generated by a nuclear burst.
FBR	Fast Burst Reactor
Flash X-ray machine	Pulsed X-ray generator used to simulate the prompt ionizing dose from a nuclear weapon.
Free-Field Environment	Environment generated from a threat weapon located at the position of the satellite or user/control terminal if it were not there.
FXR	Flash X-ray machine. Used to simulate the prompt ionizing dose from a nuclear weapon.
Hardening	The use of a design, material, or manufacturing technique that increases a component or system's ability to survive the effects of a weapon environment. Hardening includes shielding, robust structural designs, shock mounting, protective paints and coatings, electronic circumvention, electrical filtering, etc.
Hardness	A quantitative description of the resistance of a system or component to malfunction (temporary and permanent) and/or degraded performance induced by a threat weapon environment. Measured by resistance to physical quantities such as overpressure, electrical stress, etc.
Hardness Assurance	The set of screens and controls implemented to ensure that the designed-in survivability is not degraded during production.
High Altitude Burst	A detonation above 100,000 feet altitude.
Heavy Ion Flux	The natural radiation environment, either galactic or from the sun, which can cause single event effects in electronic components.
High Power Lasers	Directed at optical sensors or system sensitive materials to cause permanent damage and mission failure.
High Power Microwaves (HPM)	Directed at microwave sensitive sensors or satellite communications receivers to cause "front end" burnout. Also, there can be "Backdoor" coupling to internal components through penetrations.
High-Z material	Materials of high atomic number which strongly absorb X-rays.
Hot X-rays	The higher energy X-rays (~10-100 keV) X-rays from a nuclear burst.
IEMP	Internal Electromagnetic Pulse also sometimes referred to as Box EMP. IEMP is a result of secondary electron emission from satellite box walls caused by prompt X-rays.
Laser Jammers	Lasers directed at optical systems and sensors to cause blind spots or outages in data.
Latchup	Anomalous state of a semiconductor device which prohibits the device from responding to input signals. Can result in device burnout due to excessive flow of current within the device.
Leakage current	Current passing through a electronic device which often increases with the absorption of ionizing radiation.
LET	Linear Energy Transfer is the energy per unit length deposited along the path of an ionizing particle.
LINAC	Linear Accelerator.
Low-Z coatings	Coatings of low atomic number material used on interior box wall surfaces to absorb Compton and photoelectron currents from underlying higher-Z materials and thereby mitigate IEMP effects.
Megaton (MT)	Unit of nuclear weapon energy release equal to 10^{15} Calories
Micrometeorites and Debris	Natural and man-made material particles in earth or solar orbit which, depending or their size, can cause surface degradation or catastrophic failure of a satellite.
NBC warfare	Nuclear, Biological, and Chemical warfare
Operate Through	System meets specified functional and performance requirements while exposed to a specified threat environment (i.e., no interruption to mission in threat environment)

Overpressure	The transient pressure, usually expressed in pounds per square inch, exceeding the ambient pressure manifested in the shock or blast wave from an explosion.
Passive Defense	Countermeasures which refer to hardening or mitigation methods that apply to system components.
Photocurrent	The current caused by radiation-induced ionization.
Photocurrent Burnout	Destruction of a transistor or other electronic component by photocurrents.
Photocurrent Compensation	A radiation hardening circuit design technique which leads to equal and opposite photocurrents which cancel out.
Proliferation	The deployment of extra systems, components or pieces of equipment..
Prompt Dose	The dose produced by prompt X-rays and gamma rays from a nuclear burst.
Rad	Unit of radiation dose equal to 100 ergs/gram.
Rad Hits	Spikes of current or voltage produced in photo detectors caused by the transit of a charged particle, usually electrons, sometimes protons and heavier ions.
Radiation Design Margin (RDM)	Ratio of mean of radiation test failure levels to radiation specification level.
Rads(Si)	Dose in Rads in the material Silicon
Reconstitution	The incorporation of design features in a system or piece of equipment to facilitate repair or recovery of the affected items so the system can be returned to its normal operating capability.
Redout	Bright infrared background produced by the donation of a nuclear weapon in or just above the atmosphere which interferes with IR sensor operation.
Redundancy	The incorporation of extra components in a system or pieces of equipment that function as a back-up, or the use of alternative means of accomplishing the function of a vulnerable component.
RF Jammers	Directed at jamming communications and data links to degrade or impede mission performance. Jammers can be directed against the uplink (directed at satellite receivers), downlink (directed at user terminals) or crosslink (i.e., directed at satellite-to-satellite links).
Scintillation	Random variation in signals propagating through the natural ionosphere or nuclear burst created plasma.
SEL	Single Event Latchup; latchup caused by the transit of a single heavily ionizing charged particle.
SEU	Single Event Upset; change of state of logic circuit, memory cell, flip-flop, etc. due to the transit of a single heavily ionizing charged particle.
Shock Wave	A continuously propagated pressure pulse in the surrounding medium which may be air, water, or earth, initiated by the expansion of the hot gases produced in an explosion. A shock wave in air is generally referred to as a blast wave, because it is accompanied by strong but transient winds.
SGEMP	System Generated EMP is produced when X-rays and Gamma rays from a nuclear weapon generate Compton and photoelectrons in and around a satellite. Resulting currents can flow on spacecraft structure (Structure SGEMP) and there can be SGEMP induced currents on internal satellite cabling (cable direct drive SGEMP) as well.
Solar Flare Protons	High energy protons from storms on the sun.
Space Mine	An orbiting nuclear or conventional bomb or device which can damage a satellite upon explosion or collision.
Spot Shielding	X-ray shielding around specific vulnerable components.
STAR	System Threat Assessment Report. The authoritative threat assessment tailored for and focused on a particular U.S. defense acquisition program. Prepared by the Service intelligence agency and validated by DIA.
Survivability	The capability of a system to avoid or withstand a man-made hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission.

Susceptibility	The degree to which a device, equipment, or weapon system is open to effective attack due to one or more inherent weakness. Susceptibility is a function of operational tactics, countermeasures, probability of enemy fielding a threat, etc. Susceptibility is considered a subset of survivability.
Tap	Unit of impulse per unit area equal to gm/(cm sec)
TED	Threat Environment Description
Thermomechanical Effects	The effects associated with the sudden deposition of energy (constant volume heating) produced by the absorption of prompt X-rays from a nuclear burst.
Threat Effect Tolerance	Every component and piece of equipment has an intrinsic ability to tolerate/survive some exposure to a weapon-generated environment.
Threshold Shift	The raising or lowering of the voltage at which a digital electronic device changes state often caused by absorption of ionizing radiation.
Total Dose	The total ionizing dose (energy/unit mass) which will occur in the various parts of the system over its lifetime due to both natural and man-made sources.
Trapped Electrons	Electrons trapped in the earth's magnetosphere (the Van Allen belts)
Trapped Protons	Protons trapped in the earth's magnetosphere.
TREE	Transient Radiation Effects in Electronics
Vulnerability	The characteristics of a system that cause it to suffer a definite degradation (loss or reduction of capability to perform the designated mission) as a result of having been subjected to a certain (defined) level of effects in an unnatural (man-made) hostile environment. Vulnerability is considered a subset of survivability.

Note: Many of these definitions were obtained from 1) Glasstone, The Effects of Nuclear Weapons, 1977, 2) Defense Acquisition Acronyms & Terms--Glossary, September 1991, prepared by the Defense Systems Management College, Ft Belvoir, VA, and 3) Program Management Handbook on Nuclear Survivability, DNA-H-93-52, July 1994.

Appendix B. Applicable Documents

Source	Document	Discussion
SMC or The Aerospace Corporation library	DoD Directive 5000.1, **Defense Acquisition**, March 15, 1996	Describes DoD's integrated Acquisition Management, Requirements Generation, and Planning, Programming, and Budgeting Systems
SMC or The Aerospace Corporation library	DoD 5000.2-R, **Defense Acquisition Management Policies and Procedures**, 23 March 1998**.** See Section 4.4.1, *Survivability*	See also related subjects in Part 3 and the remainder of Part 4. See especially Section 2.2, *Intelligence Support*, and 2.3, *Requirements Evolution.*
SMC/AX	**AFMC Request for Proposal Process Guide**	Guidance for preparing an RFP
SMC/AX	**SMC Statement of Objectives (SOO) Approach**	Additional guidance for preparing an RFP that replaces the section on the Statement of Work in the previously listed document
Contact SMC/AX for the latest policy on IPD and for support in preparing RFPs that reflect the principles of IPD	**Air Force Materiel Command Guide on Integrated Product Development**, 25 May 1993 **Integrated Product Development Implementation Guide**, HQ SMC, March 1993	Guidance on implementing Integrated Product Development (IPD), a modern framework for conducting system engineering
Version 2.3.101 issued March 31, 1998. Contact SMC/AX for latest version.	**Defense Acquisition Deskbook**, prepared by OUSD (A&T) API	See Survivability General Guidelines
SMC or The Aerospace Corporation library	Mil-STD-1547B, **Electronics Parts, Materials, and Processes for Space and Launch Vehicles,**	See Appendix C and other portions related to survivability
SMC or The Aerospace Corporation library	Mil-STD-188-125, **High-Altitude Electromagnetic Pulse (HEMP) Protection for Ground-Based C4I Facilities Performing Critical, Time-urgent Missions**, 26 June 1990	Requirement as applicable.
SMC/AX	Proposed Mil-HDBK-1766, **Nuclear Hardness and Survivability Program Guidelines, Vol II Space**	In preparation.

	Systems	
Aerospace Corporation library	S. Glasstone, **The Effects of Nuclear Weapons**, 3rd Ed., U. S. Gov. Printing Office Dept. of Defense. and Energy, 1977	General text on nuclear weapons effects
Aerospace Corporation library	G. Messenger and M. Ash, **The Effects of Radiation on Electronic Systems**, New York: Van Nostrand Reinhold, 1992	General text on radiation effects on electronics
DNA	Defense Nuclear Agency Handbooks and publications	Provide nuclear effects information, general design guidelines, and test facility information
DNA or Aerospace Corporation Library	**Program Management Handbook on Nuclear Survivability**, DNA-H-93-52, July 1994	Handbook to assist program managers and their staffs with the development and acquisition of nuclear survivable systems.
Phillips Lab	Air Force Phillips Lab (including Air Force Weapons Lab) Handbooks and publications	Provide weapons effects information and general design guidelines
Phillips Lab or Aerospace Corporation Library	**USAF Handbook for the Design and Construction of HEMP/TEMPEST Shielded Facilities**, AFWL and AF/LEEEU, December 1986	Technical Design handbook for shielded facilities.
Phillips Lab or Aerospace Corporation Library	**Guidelines to Hardness Assurance for Nuclear Radiation, Blast and Thermal Effects in Systems with Moderate Requirements,** AFWL-TR- 86-26, February 1987.	Technical guideline for the development and application of hardness assurance programs for systems with low to moderate nuclear requirements.
DIA or Aerospace Library	**Electronic Warfare Threat to Satellite Communication Links-Foreign,** DIA publication DST-26110S-111-94, 31 March 1994.	Example of general satellite link jamming threat. The specific threat for a system will be identified in the system STAR (System Threat Assessment Report).

DIA or Aerospace Library	**Command, Control, Commu ications, Computers, and Intellignece (C4I) Systems and Networks; Telecommunications Networks; and Automated Information Systems Threat Environment Description (TED),** DIA publication DST-2660F-210-94, 15 January 1994.	Example of a general threat environment for information systems.