IARPA

BROAD AGENCY ANNOUNCEMENT

IARPA-BAA-09-08

I A R P A

BE THE FUTURE

SECURELY TAKING ON NEW EXECUTABLE SOFTWARE OF UNCERTAIN PROVENANCE (STONESOUP) PROGRAM

Safe and Secure Operations Office

IARPA-BAA-09-08

Release Date: SEPTEMBER 16, 2009

IARPA

BROAD AGENCY ANNOUNCEMENT: IARPA-BAA-09-08

SECURELY TAKING ON NEW EXECUTABLE SOFTWARE OF UNCERTAIN PROVENANCE (STONESOUP) PROGRAM

TABLE OF CONTENTS

PART ONE: OVERVIEW INFORMATION

This publication constitutes a Broad Agency Announcement (BAA) and sets forth research areas of interest in the area of comprehensive, automated techniques that allow end users to safely execute new software of uncertain provenance. Awards based on responses to this BAA are considered to be the result of full and open competition.

- **Federal Agency Name** – Intelligence Advanced Research Projects Activity (IARPA), Safe and Secure Operations Office
- **Funding Opportunity Title –** STONESOUP
- **Announcement Type –** Initial
- **Funding Opportunity Number – IARPA-BAA-09-08**
- **Catalog of Federal Domestic Assistance Numbers (CFDA) –** 12.910 Research and Technology Development
- **Dates**
  - Proposal Due Date: November 2, 2009
- **Anticipated Individual Awards** –Multiple awards are anticipated.
- **Types of instruments that may be awarded** – Procurement contract, grant, cooperative agreement or other transaction.
- **Agency Points of Contact**

  Dr. Carl Landwehr
  IARPA, Safe and Secure Operations Office
  ATTN: IARPA-BAA-09-08
  Office of the Director of National Intelligence
  Intelligence Advanced Research Projects Activity
  Washington, DC 20511
  Fax: 301-226-9137
  Electronic mail: dni-iarpa-baa-09-08@ugov.gov
- **Program Website:** www.iarpa.gov
- **BAA Summary:** The IARPA Securely Taking on New Executable Software of Uncertain Provenance (STONESOUP) Program is soliciting proposals to develop and demonstrate technology that provides comprehensive, automated techniques that allow end users to safely execute new software of uncertain provenance.
- **Questions:** IARPA will accept questions about the BAA until October 19, 2009. A consolidated Question and Answer response will be publicly posted every few days on the IARPA website www.iarpa.gov; no answers will go directly to the submitter. Questions about administrative, technical or contractual issues must be submitted to the BAA e-mail address at dni-iarpa-baa-09-08@ugov.gov. If e-mail is not available, fax questions to 301-226-9137, Attention: IARPA-BAA-09-08. All requests must include the name, e-mail address (if available) and phone number of a point of contact for the requested information. Do not send questions with proprietary content.

PART TWO: FULL TEXT OF ANNOUNCEMENT

Section 1: FUNDING OPPORTUNITY DESCRIPTION

The Intelligence Advanced Research Projects Activity (IARPA) often selects its research efforts through the Broad Agency Announcement (BAA) process. The BAA will appear first on the FedBizOpps website, http://www.fedbizopps.gov/, then the IARPA website at http://www.iarpa.gov. The following information is for those wishing to respond to this Program BAA.

IARPA is seeking innovative solutions for the STONESOUP Program. The use of a BAA solicitation allows a wide range of innovative ideas and concepts. The STONESOUP Program is envisioned to begin March 2010 and end by February 2014.

The IARPA Securely Taking on New Executable Software of Uncertain Provenance (STONESOUP) Program is soliciting proposals to develop and demonstrate technology that provides comprehensive, automated techniques that allow end users to safely execute new software of uncertain provenance. The envisioned technology will use advanced automated software analysis techniques to identify vulnerabilities or to assure their absence; it will combine the analysis with methods for confining software execution so that identified weaknesses cannot be exploited; and it will diversify software components so any residual vulnerabilities will be more difficult for attackers to discover or exploit.

1.A. Program Overview

Software vulnerabilities are a major security problem today. Attackers exploit these vulnerabilities to subvert computers and steal valuable information, to extort funds under threat of system damage or shutdown, or to turn an unwitting user's computer into a "bot," which the attacker can subsequently direct to attack other systems, to distribute spam, or to pursue other purposes the attacker may have.

A large fraction of these vulnerabilities originate in the source or object code of programs rather than in the software design. Yet tools to help an end user determine whether a new program is safe to run or contains exploitable vulnerabilities are largely lacking. Instead, users must typically depend on the provenance of the software they receive: Did it come from a company we trust? Was it developed using a process in which we have confidence? Are the people who built it friendly to us?

The problem with relying on provenance is that software is now developed all over the world and is often assembled out of component parts from many sources, so its origin is uncertain. It is increasingly difficult to know who built a particular software component or system, what their motivations may be, and what process they used in its construction.

This program aims to establish confidence in software based on properties determined by examining the software directly, independent of where it came from or what process was used to develop it.

Evaluating software to assure it has desired security properties is today a cumbersome and labor-intensive process. Current evaluation techniques in support of software system certification often require the creation of extensive documentation that is frequently used only by evaluators. Certification processes might not require examination of source code, where most vulnerabilities are introduced. The machine code that a computer actually executes is rarely subject to rigorous analysis. Further, software producers can issue updates and fixes at a rate faster than current processes can evaluate their effects.

Recently, a market has developed in tools that can automatically detect weaknesses in source or object code programs. However, while current tools show promise, they typically generate reports of weaknesses that are intended for manual review by a software developer or security expert, not an end user. Moreover, these tools produce significant numbers of false positives, greatly magnifying the effort required to triage vulnerability reports, and false negatives, allowing vulnerabilities to slip through the cracks.

The goal of the STONESOUP program is to develop and demonstrate technology that provides comprehensive, automated techniques that allow end users to safely execute new software of uncertain provenance. The envisioned technology will use advanced automated software analysis techniques to identify vulnerabilities or to assure their absence; it will combine the analysis with methods for confining software execution so that identified weaknesses cannot be exploited; and it will diversify software components so any residual vulnerabilities will be more difficult for attackers to discover or exploit. The combination of these techniques can provide true defense-in-depth against attempts to exploit vulnerable software.

Tools that can operate on programs written in common, type-safe languages, specifically C# or Java (source or bytecode), in legacy, harder-to-analyze languages, specifically C or C++, as well as object code programs available only in binary format for x86 (Windows or Linux), are of interest to the program.

Background

Most modern programming languages include a range of features to help programmers construct today's large, complex software systems. For example, abstraction and encapsulation, as embodied by functions, classes, and modules, help isolate components of a system. As another example, type and memory safe languages prevent undefined and potentially harmful errors (e.g., buffer overflows). These kinds of language-based features are enforced by a combination of the language compiler and run-time system, and a careful, thoughtful programmer can gain tremendous benefit from them.

Unfortunately, the presence of these language features, while helpful, cannot guarantee the absence of security vulnerabilities that could be exploited by a malicious adversary. For example, even a type and memory safe program may allow logic errors that open up software to exploitation. Thus, it is left up to programmers to code defensively against such vulnerabilities. However, this is not an easy task. Many programmers are unaware of how to write secure code. Even those who do know often accidentally introduce bugs into their code, and some of those bugs later turn out to be vulnerabilities. Even worse, new techniques for discovering and exploiting vulnerabilities are always being invented. Hence today's secure software might turn out to have weaknesses that only become apparent in the future.

Many recently developed source and object code scanners, both research and commercial, have demonstrated that they can find thousands of security vulnerabilities, including null pointer errors, buffer overflows, race conditions, format string vulnerabilities, and others. In theory, it is possible to build tools that can guarantee the absence of vulnerabilities of a particular sort, but in practice today such a guarantee comes only with a large number of false positives – trouble reports that do not actually correspond to vulnerabilities. To reduce the rate of false positive reports to an acceptable level, tools typically discard reports that algorithms indicate are relatively unlikely to cause trouble – consequently introducing false negatives (vulnerabilities that should be reported, but are not).

Finally, these tools are designed for software developers to use. They produce error reports that are typically understandable only to programmers, and remediating detected problems usually requires modifying the program source code, which is not a task end users can easily undertake. With malicious

adversaries actively trying to exploit weaknesses that have been missed by the tools or the programmer, this "best effort" approach to finding and eliminating vulnerabilities falls short.

While source and object code analysis tools have been making great strides, two other complementary technologies have also been advancing: approaches to confine security vulnerabilities, and approaches to diversify software to make unknown vulnerabilities harder to exploit.

Confinement refers to mechanisms that allow vulnerabilities to be present in the program's source or object code, but prevent those vulnerabilities from being exploited at run time. A canonical example is operating system (OS)-level process separation, which isolates processes on a system and prevents them from interfering with each other in arbitrary ways. For example, one process is not allowed to access the (unshared) memory of a different process. As with type and memory safety, this is a fairly coarse property, and it does not in itself eliminate security vulnerabilities. A more general class of security policy can be enforced by inline reference monitors (IRMs), which observe software as it is running and stop the software from performing particular unsafe operations. A security policy can be specified for an IRM (for example, a process sends no messages after reading a particular file), and code can be inserted to enforce that policy throughout a program. This approach draws on earlier work on Software Fault Isolation (SFI), in which object code is rewritten to prevent accesses to memory outside the space allocated to a particular component.

These regimes leave open the question of how the program behaves when an attempted policy violation occurs. SFI typically operates in a failure oblivious mode -- the program continues to run as though no failure had occurred, but since it will not have read the data it was attempting to access, its future behavior may become unpredictable. Alternatively, the enforcement may adopt a fail stop approach: when the policy violation occurs, the current process is aborted, and the enclosing context must deal with the termination event. This prevents vulnerabilities from being exploited directly, but it introduces the possibility of denial of service. An OS that terminates a process that causes a memory fault through an invalid address reference or an attempt to invoke a privileged instruction from user mode is operating in a fail-stop regime.

Since confinement typically occurs at run time, it can be much more precise than source or object code analysis. At the time a confinement mechanism is invoked, information is available about the current execution environment that is difficult or impossible to pre-compute, and the confinement mechanism can use this information to pinpoint the violation and determine an appropriate course of action. In contrast, source and object code analysis is typically concerned with preventing problems in all possible runs, so it must be more conservative in its analysis. Yet confinement leaves vulnerabilities latent at run-time, and being forced to choose between fail-stop and failure oblivious behaviors is not ideal.

Another approach to dealing with security vulnerabilities is diversification, which means changing the way a program executes in order to make it much harder for an attacker to take advantage of a vulnerability. For many kinds of attacks to succeed, the attacker needs to determine the relative or absolute memory locations of, for example, the stack or heap for the current context, or the locations of shared library routines that the attacker may want to call. If these locations are fixed or easily predicted across many different computers, an attacker can afford to invest significant resources in determining those locations. Some diversification strategies seek to alter the memory structure of programs so that even if the attacker finds an exploitable vulnerability in one system, it will be difficult to determine how to exploit the same vulnerability on a different computer, on the same machine after a reboot, or potentially even in a different process running the same application on the same machine.

Address space layout randomization (ASLR) is a diversification technique currently available for use in Microsoft, Linux, and MacOS operating systems in various forms. On each run (each reboot in some cases), ASLR can relocate critical data such as locations of shared library functions so that attacks that

succeeded on the prior bootload are unlikely to work on the newly booted system. Some compilers now include options to generate code that will randomize the location of the heap or the stack base as well, another form of diversification. Some techniques, such as adding "canary" elements to stacks, combine diversification and confinement. The canary value (to be checked on a function return to assure the stack has not been overwritten) may be diversified so that the attacker cannot easily mimic it and thereby defeat the mechanism. None of these methods, properly implemented, should alter the semantics of the program or system in question on normal (non-malicious) inputs.

Just like analysis and confinement, diversification has its limits. While diversification makes it harder to exploit an existing vulnerability, it does not eliminate the vulnerability itself, and clever attackers have developed ways to defeat diversification. For example, "landing pads" can be added to exploit code to make it less sensitive to the location at which it is loaded. Some vulnerabilities can reveal the address of the stack, negating the benefit of relocating it. And data-only attacks are insensitive to the location of program code. However, while diversification is not perfect, it does increase the requirements for successful attacks and is an important component of a defense-in-depth approach.

Program Research Focus

Analysis, confinement, and diversification methods have made major advances in recent years, and all three have shown effectiveness in reducing vulnerabilities in practice. However, these techniques are still limited in their scope and operate in stovepipes. For example, one tool might address buffer overflows, and an independent tool might address format-string vulnerabilities. Finally, these techniques are typically used independently, and they do not interoperate. For example, vulnerabilities that are missed by a code analysis tool will likely remain in the code, subject neither to confinement nor to diversification. The result is that even if analysis, confinement, and diversification are used together to address a number of vulnerabilities, the result is a patchwork with many holes in it, and the ultimate benefit is hard to characterize.

STONESOUP seeks solutions that substantially reduce vulnerability to malicious exploitation of software flaws by (a) extending the scope and capability of approaches for analysis, confinement, and diversification; (b) addressing a wide range of security vulnerabilities within the same framework; and (c) combining analysis, confinement, and diversification to leverage the strengths and weaknesses of each approach. The major advance sought is to provide comprehensive, automated techniques for vulnerability reduction in software of uncertain provenance.

Analysis - Advances Sought

A recent study[1] (Merced, 2009) of several current vulnerability detection tools showed that roughly 40% of inserted vulnerabilities were not detected by any of the studied tools. The study's test inputs were short segments of C, C++, and Java code incorporating specific vulnerabilities. Further, tools covered different, partially overlapping, subsets of the space of software vulnerabilities. So, to assure detection of even half of the tested weaknesses with today's tools it would be necessary to process the software with several different tools. STONESOUP seeks advances in analysis technology so that a single tool can achieve the coverage goals called for in the program milestones.

Today's tools generate reports intended for software developers. The STONESOUP program seeks to develop tools that operate without human interaction. A tool should either reject input provided to it or report the presence and absence of various types of vulnerabilities and confine or diversify those vulnerabilities it finds, so that the software is safe to run. The argument that the code is not subject to a

[1] Merced, J. (2009, June). *Source Code Analysis Tool Evalution Briefing*. Available at STONESOUP BAA website: http://www.iarpa.gov/stonesoup_Merced_DHSAWGbrief.pdf

particular set of vulnerabilities may depend on the (automated) confinement and diversification mechanisms described below. While the baseline program goals are to be met without the use of human interaction, some level of human assistance, such as auxiliary annotations (introduced by the proposer) may be permitted to demonstrate performance that exceeds the baseline.

Confinement - Advances Sought

Confinement of undesired effects of a program is traditionally achieved through a combination of software and hardware mechanisms. For example, a program that generates an out-of-bounds memory reference, if executed on a machine using a real addressing mode, might succeed in reading or writing memory that had been allocated to another process. The same memory reference, if executed in a virtual addressing mode with the page and segment tables properly set up, would simply cause an addressing exception or a page fault, which the supervisor and operating system could handle in an appropriate way, e.g., by aborting the process (fail-stop) or creating a new virtual memory region and supporting the read or write operation (failure oblivious).

Systems have also been proposed and implemented that take a pure software approach to confinement. A compiler providing an IRM capability might insert extra instructions to check that the memory reference is in bounds and, if not, signal an error. Tools like Purify[2] and Valgrind[3] transform code to, among other things, ensure reads and writes to buffers are within bounds, and that allocated memory is not leaked. Approaches implemented purely in software tend to be less efficient than those that rely on hardware, though they can also be finer-grained and more flexible.

The STONESOUP program seeks effective combinations of confinement and performance, and to broaden the scope of vulnerabilities that can be ameliorated through confinement. Portable, software-only approaches are preferred, provided they can meet performance requirements. Proposers may also develop confinement mechanisms that take advantage of particular hardware or operating system constructs for performance. The operating system and architecture should be selected from widely available, commodity systems based on the x86 instruction set, and popular operating systems, especially including Windows and Linux. Proposers are also encouraged to consider whether, when a policy violation is detected, alternatives preferable to either fail-stop or failure oblivious operation may be available.

Diversification - Advances Sought

Arguably the most widely used form of diversification today is address-space layout randomization. Other ideas that have been proposed include flipping the direction of stack growth, randomizing the locations of heap allocations, and randomly padding heap allocation requests. In some cases, replication or n-version programming has been suggested, in which multiple copies of an executable are run, each suitably randomized in some way, and then a "vote" is taken to decide which path the program will take. In a security context, this idea means that an attacker must compromise a majority of replicas to gain an advantage, which is presumably more difficult than compromising a single program instance.

The diversification approaches just mentioned aim to compensate for a limited set of weaknesses. The STONESOUP program seeks to increase the range of security vulnerabilities that diversification can protect against. As part of the research, the scope of a particular diversification technique should be identified, in terms of the weaknesses it aims to address. Measurements or estimates of a diversification strategy's effectiveness are sought, e.g., probabilistic arguments based on explicit assumptions. Performance of diversification strategies is also important, and the resources consumed by a diversified

[2]IBM Rational Purify. http://www-01.ibm.com/software/awdtools/purify/
[3] Valgrind Home Page. http://valgrind.org

program should be within a reasonable factor of the original program, as specified in Section 1.B. If replication is a part of a proposed diversification strategy, an argument should be made that the amount of replication is achievable on commodity platform (e.g., multicore CPUs may provide an efficient basis for replication).

Combining analysis, confinement, diversification

Analysis, confinement, and diversification each address different facets of the software security problem: Analysis can provide strong guarantees about the absence of vulnerabilities in all runs, though only for a limited set of vulnerabilities. Confinement can guarantee that a vulnerable software instruction cannot violate the bounds imposed by the confinement mechanism, but it introduces the problem of what to do when a vulnerability is detected at run time. Diversification makes vulnerabilities harder to exploit, and is attractive for addressing unexpected vulnerabilities or those that are not practical to address with analysis or confinement, and for providing additional assurance in general.

The STONESOUP program seeks solutions that combine analysis, confinement, and diversification to leverage the strengths of all three approaches in a single, comprehensive framework. Solutions should indicate the quantity and quality of analysis/confinement/diversification provided, so that an end user can understand the extent of the assurance provided.

Vulnerabilities

The aim of STONESOUP is to reduce the vulnerability of software to attacks that compromise security. There are many different known sets of security vulnerabilities, and the STONESOUP program seeks comprehensive solutions that ameliorate a range of vulnerabilities in a single framework. Vulnerabilities of interest include, but are not necessarily limited to:

- Buffer overflows/memory safety errors
- Race conditions, atomicity violations, TOCTTOU (time of check to time of use) vulnerabilities
- Integer overflow, underflow, and sign conversion errors
- Null pointer errors
- Resource drains that may be subject to attack (e.g., memory or file handle leaks)
- Other memory errors (double frees, use after free, uninitialized memory use)
- Insufficient access control checks/incomplete mediation
- Tainted data/input validation errors (e.g., format string vulnerabilities, lack of checking on command strings sent to OS, insufficient restrictions on input file names)
- Unhandled exceptions or returned error status codes
- Leaks of confidential information

Only certain of these vulnerabilities apply to particular domains. (For example, buffer overflows are an issue for C, C++, and binaries, but likely not for Java or C#.) Proposals need not address all the vulnerabilities listed above; see section I.B for more detailed vulnerability lists on which performance will be judged. Proposals may also address additional vulnerabilities that are not on the list, in which case there should be a justification of the importance of the additional vulnerabilities.

The STONESOUP program aims to eliminate the effects of vulnerabilities that are inadvertently included in software programs. Since a functional specification is not required for the software to be processed, it will not generally be possible to detect incorrect or malicious logic such as trapdoors, logic bombs, or incorrect implementation of cryptographic primitives.

Assessment

Efforts will be judged against a range of test inputs and by red teaming, according to the phase of the program, as specified in Section 1.B. An Evaluation Team will develop test inputs that include a range of small, synthetic test cases targeted to particular vulnerabilities, as well as larger software systems. Some of the test inputs (of both sizes) will be made available to performers at the program kickoff meeting, and some will be reserved for testing at project milestones. Offerors are also welcome to propose to generate their own test inputs for demonstration purposes. The NIST Common Weakness Enumeration (CWE) defines classes of vulnerabilities that may be used in defining test data for the program. Near the end of each program phase, the Evaluation Team will visit each research site to provide test data and witness tests conducted on the tools under development.

Specific measures of interest include:

- The number of vulnerabilities rendered inert by an integrated analysis/confinement/diversification approach
- Performance of the software to be run, e.g., with modifications for confinement and diversification
- Behavior of the software to be run: inputs that have no vulnerabilities should not execute differently before or after modification, except possibly either performance changes or differences due to undefined or underspecified semantics of the original program (e.g., C or C++ behavior that is system-dependent)

The specific test regime that will be used to evaluate program progress is presented in Section 1.B. These assessments will involve many test cases of small code snippets, but also some tests on larger software systems. For the larger test cases (e.g., 10,000 source lines of code in Phase 1 and up to 500,000 sources lines in Phase 3) ground truth, in the sense of a known complete list of vulnerabilities in the input, will likely not be available. Vulnerabilities may be seeded in these samples, but tools may detect unseeded, previously unknown, vulnerabilities as well. In such situations, the Evaluation Team will provide rationalized assessments of the performance of different tools on the same test inputs based on their knowledge and experience.

1.B. Program Milestones and Metrics

The Government will use the following Program Milestones and Metrics to evaluate the effectiveness of proposed solutions in achieving the stated program objectives, and to determine whether satisfactory progress is being made to warrant continued funding of the program. These metrics are intended to bound the scope of effort, while affording maximum flexibility, creativity, and innovation in proposing solutions to the stated problem.

In the text below, language classes are referred to by letters as follows:

A – Type-safe languages (Java, C#)
B – Type-unsafe languages (C, C++)
C – Binaries (x86, Windows or Linux)

Phase 1 Milestones

Proposers must identify the programming language or languages they will accept as input and at least six vulnerability sets, drawn from the following lists, that they will address during the course of the program. The programming language(s) must be selected from those listed in class A, B, or C above, and the

vulnerability sets should be drawn from the lists below[4]. Following each vulnerability set is a small set of sample CWE entries in parentheses (definitions of which can be found at cwe.mitre.org) illustrating the vulnerability set. These examples are supplied for illustration purposes; proposals should address the general set, and not be restricted to the particular examples listed. Near the end of Phase 1, each performer will be required to identify the two vulnerability sets on which their tool's performance will be measured for that Phase. Offerors may propose to address a single programming language, two (or more) programming languages in a single class, or any combination of programming languages in different classes. Proposals that address programming languages in more than one class should include a rationale for how the six (or more) selected vulnerability sets were chosen.

Each proposal should describe the strategy to be used to allow both the number of sets of vulnerabilities handled and the maximum input program size to grow as the program proceeds through its phases. Offerors should consider whether it will be more effective to focus sharply on two specific vulnerability sets in Phase 1 and then two more in Phase 2, for example, or to structure the effort so that a larger collection of vulnerability sets is explored in parallel, with the vulnerability sets against which the best performance has been achieved by the end of Phase 1 being selected as the basis for the initial evaluation.

Vulnerability List for Language Class A:

- Set A1. Number handling (e.g., integer overflow, underflow, sign conversion errors: CWE #190, #191)
- Set A2. Tainted data/input validation errors (e.g., CWE #24, #78)
- Set A3. Error handling (e.g., unhandled exceptions/error status codes : CWE #248, #252)
- Set A4. Resource drains (e.g.,failure to release memory, data structures, devices: CWE #400, #404)
- Set A5. SQL injection / command injection (e.g., CWE #78, #89)
- Set A6. Concurrency handling (e.g., race conditions, thread safety :CWE #362, #366)

Vulnerability List for Language Class B:

- Set B1. Number handling (e.g., integer overflow, underflow, and sign conversion errors: CWE #190, #191)
- Set B2. Tainted data/input validation errors (e.g., CWE #78, #134)
- Set B3. Error handling (e.g., unhandled exceptions/error status codes: CWE #248, #252)
- Set B4. Resource drains (e.g.,failure to release memory, data structures, devices: CWE #400, #404)
- Set B5. SQL injection / command injection (e.g., CWE #78, #89)
- Set B6. Concurrency handling (e.g., race conditions, thread safety :CWE #362, #366)
- Set B7. Buffer overflows/underflows/out of bounds accesses/memory safety errors (e.g., CWE #121, #122)
- Set B8 Null pointer errors (e.g., CWE #476)

Vulnerability List for Language Class C:

- Set C1. Number handling (e.g., integer overflow, underflow, and sign conversion errors: CWE #190, #191)
- Set C2. Tainted data/input validation errors (e.g., CWE #78, #134)
- Set C3. Error handling (e.g., unhandled exceptions/error status codes: CWE #248, #252)
- Set C4. Resource drains (e.g.,failure to release memory, data structures, devices: CWE #400, #404)
- Set C5. SQL injection / command injection (e.g., CWE #78, #89)
- Set C6. Concurrency handling (e.g., race conditions, thread safety :CWE #362, #366)

[4] Offerors may propose additional vulnerability sets not included in these lists, but they will need to provide a justification for including them.

Set C7. Buffer overflows/underflows/out of bounds accesses/memory safety errors (e.g., CWE #121, #122)
Set C8. Null pointer errors (e.g., CWE #476)

Tools developed for a specific programming language should identify vulnerabilities, confine the effects of identified vulnerabilities, and diversify software to render unidentified vulnerabilities harder to exploit. A tool may also fail to process (reject) some fraction of the input data. The maximum size of test programs to be used in Phase 1 Test & Evaluation will be approximately 10,000 lines of source. In this and subsequent phases, the maximum size object file test cases will be generated by compiling source programs of the specified maximum size for that phase. Phase 1 performance targets are provided in the table below. Achievement of these targets will be evaluated in Month 16 of the program.

Table 1: STONESOUP Phase 1 Metrics.

Language Class	Percent of submitted programs successfully processed	Percent of seeded vulnerabilities rendered unexploitable
A	100	75
B	90	75
C	75	75

Phase 2 Milestones

Near the end of Phase 2, each performer will specify two additional vulnerability sets from the six identified at the outset, which, together with the two already identified in Phase 1, will be used to assess Phase 2 results. Data sets including vulnerabilities in both the Phase 1 and Phase 2 sets will be developed by the Evaluation Team. Performance will be characterized separately for the Phase 1 and Phase 2 vulnerability sets. Approximate maximum sizes of test programs to be used in Phase 2 Test & Evaluation will be 100,000 lines of source for both Phase 1 and Phase 2 vulnerability sets. Performance targets are provided in the table below. Achievement of these targets will be evaluated in Month 28 of the program.

Table 2: STONESOUP Phase 2 Metrics.

Language Class	Percent of submitted programs successfully processed	Percent of seeded vulnerabilities rendered unexploitable
A	100	90 (Phase 1 vulnerability sets) 80 (Phase 2 vulnerability sets)
B	90	90 (Phase 1 vulnerability sets) 80 (Phase 2 vulnerability sets)
C	75	90 (Phase 1 vulnerability sets) 80 (Phase 2 vulnerability sets)

Phase 3 Milestones

Near the end of Phase 3, the Evaluation Team will visit each active site to test the full set of six vulnerability sets. In addition, performance of the processed programs will be compared to performance of the unprocessed versions of the same software. In all cases, the performance target will be no more than a 10% increase in running time for the processed software in relation to the unprocessed software. A red team will assess the work factor added by the diversification approach and provide a check on the analysis and confinement approaches. Approximate maximum sizes of test programs to be used in Phase 3 Test & Evaluation will be 500,000 lines of source for all six vulnerability classes specified. Performance targets are provided in the table below. Achievement of these targets will be evaluated in Month 46 of the program.

Table 3: STONESOUP Phase 3 Metrics.

Language Class	Percent of submitted programs successfully processed	Percent of seeded vulnerabilities rendered unexploitable
A	100	95 (Phase 1&2 vulnerability sets) 90 (Phase 3 vulnerability sets)
B	90	95 (Phase 1&2 vulnerability sets) 90 (Phase 3 vulnerability sets)
C	75	95 (Phase 1&2 vulnerability sets) 90 (Phase 3 vulnerability sets)

In order to increase the likelihood that the above milestones will be met, several Progress Waypoints are outlined below. Offerors are expected to address each of these waypoints in their proposals and provide specific metrics and deliverables in their proposals at 6-month intervals that will enable the program manager to assess their progress. The Program Manager and advisors will use these waypoints to assess progress toward program goals and make course corrections as needed to ensure program success.

Table 4 presents a timeline of both program waypoints and program milestones.

Table 4: STONESOUP Program Waypoints and Milestones.

Date and Event Type	Description	Requirement	Intent
Month 1 Milestone	Phase 1 Kickoff Meeting	Kickoff meeting, schedule, staffing, technical discussion	Ensure common understanding of program goals, structure, metrics, evaluations, roles. Distribute initial vulnerability test sets.
Month 6 Waypoint	Site Visit 1	Attendance by Principal Investigators and Key Personnel	Assess progress of research based on offeror-proposed metrics as specified in proposals

Month 12 Waypoint	STONESOUP Principal Investigator's Meeting	Attendance by Principal Investigators and Key Personnel	Preliminary report of research results on supplied test data.
Month 16 Milestone	a. Site Visit 2 b. Evaluation against Phase 1 performance targets	a.Attendance by Principal Investigators and Key Personnel b. Achievement of Phase 1 Goals	Performers will present preliminary findings from research. Prototypes will be subjected to Government T&E against Phase 1 metrics. Researchers will be expected to have demonstrated the technical feasibility of their solution . Results will be a key factor in determining whether a performer continues to Phase 2
Month 18 Milestone	Phase 1 Final Report	Delivery of final report documenting Phase 1 results Delivery of final Phase 1 software	Capture Phase 1 technical results of each research effort
Month 19 Milestone	Phase 2 Kickoff Meeting	Attendance by Principal Investigators and Key Personnel	Ensure common understanding of program goals, structure, metrics, evaluations, roles. Distribute initial Phase 2 vulnerability test sets.
Month 24 Waypoint	STONESOUP Principal Investigator's Meeting	Attendance by Principal Investigators and Key Personnel	Assess progress of research based on offeror-proposed metrics as specified in proposals
Month 28 Milestone	a. Site Visit 3 b. Evaluation against Phase 2 performance targets	a. Attendance by Principal Investigators and Key Personnel b. Achievement of Phase 2 Goals	Performers will present preliminary findings from research. Prototypes will be subjected to Government T&E against Phase 2 metrics. Researchers will be expected to have demonstrated the effectiveness of their approach to handling an expanded number of software weaknesses and larger program sizes. Results will be a key factor in determining whether a performer continues to Phase 3
Month 30 Milestone	Phase 2 Final Report	Delivery of report documenting Phase 2 results Delivery of final Phase 2 software	Capture Phase 2 results for each research effort

Month 31 Milestone	Phase 3 Kickoff Meeting	Attendance by Principal Investigators and Key Personnel	Ensure common understanding of program goals, structure, metrics, evaluations, roles. Distribute initial Phase 3 vulnerability test sets. Introduce red team.
Month 36 Waypoint	Site visit 4	Attendance by Principal Investigators and Key Personnel	Assess progress of research based on offeror-proposed metrics as specified in proposals
Month 42 Waypoint	STONESOUP Principal Investigator's Meeting	Attendance by Principal Investigators and Key Personnel	Preliminary report of research results
Month 46 Milestone	a. Site Visit 5 b. Evaluation against Phase 3 performance targets	a. Attendance by Principal Investigators and Key Personnel b. Achievement of Phase 3 Goals	Performers will present preliminary findings from research. Prototypes will be subjected to Government T&E against Phase 3 metrics. Researchers will be expected to have demonstrated the effectiveness of their approach to enhancing usability and performance.
Month 48 Milestone	STONESOUP Final Report	Delivery of report documenting overall program results Delivery of final Phase 3 software	Capture program research results for each research effort

SECTION 2: AWARD INFORMATION

The STONESOUP Program is envisioned as a 4-year effort consisting of three consecutive phases that is intended to begin March 2010. Phase 1 is planned as a base period of 18 months; Phase 2 is planned as a possible option period of 12 months; Phase 3 is planned as a second possible option period of 18 months. Funding for option years will depend upon program priorities, performance, the availability of funding and IARPA priorities.

Potential participants in Phase 2 will be those teams that have made significant progress in Phase 1 and have correctly understood and contributed to the overarching goals of the Program. Teams that offer only minor enhancements to the current state of the art will not be invited to continue with the Program. Phase 2 will target an expanded number of software weaknesses and larger program sizes.

Similarly, potential participants in Phase 3 will be those teams that have made significant progress in Phase 2 and have demonstrated a continuing contribution to the overarching goals of the Program. Teams that fail to make significant progress in Phase 2 will not be invited to continue with the Program. Phase 3 will target usability and performance.

Multiple Phase 1 awards are anticipated. The amount of resources made available under this BAA will depend on the quality of the proposals received and the availability of funds.

The Government reserves the right to select for negotiation all, some, one or none of the proposals received in response to this solicitation and to make awards without discussions with offerors. The Government also reserves the right to conduct discussions if the Source Selection Authority determines them to be necessary. If the proposed effort is inherently divisible and nothing is gained from the aggregation, offerors should consider submitting it as multiple independent efforts. IARPA reserves the right to accept proposals in their entirety or to select only portions of proposals for award. In the event that IARPA desires to award only portions of a proposal, negotiations may be opened with that offeror.

Awards under this BAA will be made to offerors on the basis of the evaluation criteria listed in 5.A, program balance, and availability of funds. Proposals identified for negotiation may result in a procurement contract, grant, cooperative agreement, or other transaction agreement (OTA). However, the Government reserves the right to negotiate the type of award instrument it determines appropriate under the circumstances.

Offerors whose proposals are accepted for funding will be contacted before award to obtain additional information required for award. The Government may establish a deadline for the close of fact-finding and negotiations that allows a reasonable time for the award of a contract. Offerors that are not responsive to government deadlines established and communicated with the request, may be removed from award consideration. Offerors may also be removed from award consideration should the parties fail to reach agreement on contract terms, conditions, and cost/price within a reasonable time.

2.A. Other Transaction Agreements (OTA)

Other Transaction for Research. A legal instrument, consistent with 10 U.S.C. 2371, which may be used when the use of a contract, grant, or cooperative agreement is not feasible or appropriate for basic, applied, and advanced research projects. The research covered under another transaction shall not be duplicative of research being conducted under an existing DOD program. To the maximum extent practicable, other transactions shall provide for a 50/50 cost share between the Government and the offeror. An offeror's cost share may take the form of cash, independent research and development (IR&D), foregone intellectual property rights, equipment, or access to unique facilities, as well as others. Due to the extent of cost share, and the fact that an other transaction does not qualify as a "funding agreement" as defined at 37 CFR 401.2(a), the intellectual property provisions of an other transaction can be negotiated to provide expanded protection to an offeror's intellectual property. No fee or profit is allowed on other transactions.

SECTION 3: ELIGIBILITY INFORMATION

3.A. Eligible Applicants

All responsible sources capable of satisfying the Government's needs may submit a proposal. Historically Black Colleges and Universities (HBCUs), Small Businesses, Small Disadvantaged Businesses and Minority Institutions (MIs) are encouraged to submit proposals and join others in submitting proposals; however, no portion of this announcement will be set aside for these organizations' participation due to the impracticality of reserving discrete or severable areas for exclusive competition among these entities. Other Government Agencies, Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), and any other similar type of organization that has a special relationship with the Government, that gives them access to privileged and/or proprietary information or access to Government equipment or real property, are not eligible to submit proposals under this BAA or participate as team members under proposals submitted by eligible entities.

Only U.S. organizations or institutions[5] may prime and submit proposals to the STONESOUP BAA. Foreign participants and/or individuals may work on the effort to the extent participants comply with all applicable Non-Disclosure Agreements, Security Regulations, Export Control Laws, and other governing statutes applicable under the circumstances. Proposers are expected to ensure that the efforts of foreign participants do not either directly or indirectly compromise the laws of the United States, nor its security interests. As such, proposers should carefully consider the roles and responsibilities of foreign participants as they pursue teaming arrangements to propose to the STONESOUP BAA.

The lead Principal Investigator (PI) on each effort must be a U. S. person[6]. This eligibility requirement does NOT apply to other research effort team members. The PI shall be capable of individually representing the research activity in depth in front of IARPA and/or technical peers, and shall provide the primary vision and direction for the research.

3.A.1. Procurement Integrity, Standards of Conduct, Ethical Considerations and Organizational Conflicts of Interest (OCI)

"Organizational conflict of interest" means that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the Government, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage.

If a prospective offeror, or any of its proposed subcontractor teammates, believes that a potential conflict of interest exists or may exist (whether organizational or otherwise), the offeror should promptly raise the issue with IARPA and submit a waiver request by e-mail to the mailbox address for this BAA at dni-iarpa-baa-09-08@ugov.gov. All waiver requests must be submitted through the offeror, regardless of whether the waiver request addresses a potential OCI for the offeror or one of its subcontractor teammates. A potential conflict of interest includes but is not limited to any instance where an offeror, or any of its proposed subcontractor teammates, is providing either scientific, engineering and technical assistance (SETA) or technical consultation to IARPA. In all cases, the waiver request shall identify the contract under which the SETA or consultant support is being provided. Without a waiver from the IARPA Director, neither an offeror, nor its proposed subcontractor teammates, can simultaneously provide SETA support or technical consultation to IARPA and compete or perform as a Performer under this solicitation.

All facts relevant to the existence of the potential conflict of interest, real or perceived, should be disclosed in the waiver request. The request should also include a proposed plan to avoid, neutralize or mitigate such conflict. The offeror, or subcontractor teammate as appropriate, shall certify that all information provided is accurate and complete, and that all potential conflicts, real or perceived, have been disclosed. It is recommended that an offeror submit this request as soon as possible after release of the BAA before significant time and effort are expended in preparing a proposal. If, in the sole opinion of the Government, after full consideration of the circumstances, the conflict situation cannot be resolved,

[5] "U.S. organizations or institutions" means any corporation, business association, partnership, trust, academic institution, society or any other entity or group that is incorporated or organized to do business in the United States. It specifically excludes any foreign corporation, business association, partnership, trust, academic institution, society or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments and any agency or subdivision of foreign governments.

[6] U.S. person means a person who is a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). It does not include any foreign person as defined in 22 C.F.R. §120.16.

the request for waiver will be denied, and any proposal submitted by the offeror that includes the conflicted entity will be withdrawn from consideration for award.

As part of their proposal, offerors who have identified any potential conflicts of interest shall include either an approved waiver signed by the IARPA Director or a copy of their waiver request. Otherwise, offerors should certify that neither they nor their subcontractor teammates have any potential conflicts of interest, real or perceived.

If, at any time during the solicitation or award process, IARPA discovers that an offeror has a potential conflict of interest, and no waiver request has been submitted by the offeror, IARPA reserves the right to immediately withdraw the proposal from further consideration for award.

3.B. US Academic Organizations

According to Executive Order 12333, as amended, paragraph 2.7, "Elements of the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized intelligence purposes. Contracts or arrangements with academic institutions may be undertaken only with the consent of appropriate officials of the institution."

It is highly recommended that offerors submit with their proposal a completed and signed Academic Institution Acknowledgement Letter for each U.S. academic organization that is a part of their team, whether the academic organization is serving in the role of prime, or a subcontractor or consultant at any tier of their team. A template of the Academic Institution Acknowledgement Letter is enclosed in this BAA at Appendix A. It should be noted that the completed form must be signed by an appropriate senior official from the institution, typically the President, Chancellor, Provost, or other appropriately designated official. Note that this paperwork **must** be completed before IARPA can enter into any negotiations with any offeror when a U.S. academic organization is a part of its team.

3.C. Cost Sharing/Matching

Cost sharing is not required and is not an evaluation criterion; however, cost sharing will be carefully considered and may be required where there is an applicable statutory or regulatory condition relating to the selected award instrument (e.g., for any other transactions under the authority of 10 U.S.C. § 2371). Cost sharing is encouraged where there is a reasonable probability of a potential commercial application related to the proposed research and development effort.

3.D. Other Eligibility Criteria

3.D.1. Collaboration Efforts

Collaborative efforts and teaming arrangements among potential performers are strongly encouraged. Specific content, communications, networking and team formations are the sole responsibility of the participants.

SECTION 4: APPLICATION AND SUBMISSION INFORMATION

This notice constitutes the total BAA and contains all information required to submit a proposal. No additional forms, kits, or other materials are required.

4.A. Content and Form of Application Submission

4.A.1. Proposal Information

Offerors are required to submit proposals by the time and date specified in section 4.C.1. in order to be considered during the initial round of selections. IARPA may evaluate proposals received after this date for a period of up to one year from the date of initial posting on FedBizOpps. Selection remains contingent on availability of funds.

The typical proposal should express a consolidated effort in support of one or more related technical concepts or ideas. Disjointed efforts should not be included in a single proposal.

Offerors should submit proposals for a Phase 1 Base Period of 18-months plus a possible Phase 2 Option Period of 12 months and a possible Phase 3 Option Period of 18 months.

The Government intends to use employees of Omen, LLC, Teknoworks, Inc., and The University Of Maryland, College Park to provide expert advice regarding portions of the proposals submitted to the Government. Booz Allen Hamilton will also provide logistical support in carrying out the evaluation process. These personnel will have signed and be subject to the terms and conditions of non-disclosure agreements. By submission of its proposal, an offeror agrees that its proposal information may be disclosed to employees of these organizations for the limited purpose stated above. If offerors do not send notice of objection to this arrangement, the Government will assume consent to the use of contractor support personnel in assisting the review of submittal(s) under this BAA.

Only Government personnel will make evaluation and award determinations under this BAA.

All administrative correspondence and questions regarding this solicitation should be directed by e-mail to dni-iarpa-baa-09-08@ugov.gov. Proposals must be mailed to the address provided in Section 4.C.2. Proposals may **not** be submitted by hand, e-mail or fax; proposals received in this manner will be disregarded. See below for proposal submission instructions.

Offerors must submit two hard copies and one soft copy of their proposals: one original hard copy with original signatures; one hard copy with original or copied signatures; and 1 electronic copy with Volume 1, Volume 2 and any permitted, additional information (.pdf format preferred) on a CD-ROM. Both hard copies and the CD must be clearly labeled with the following information: IARPA-BAA-09-08, the offeror's organization, the proposal title (short title recommended), and copy # of #.

4.A.2. Proposal Format

All proposals must be in the format given below. Nonconforming proposals may be rejected without review. Proposals shall consist of two volumes: "Volume 1 - Technical and Management Proposal" and "Volume 2 - Cost Proposal." All pages shall be printed on 8-1/2 by 11 inch paper with type not smaller than 12 point. Smaller font may be used for figures, tables and charts. The page limitation for full proposals includes all figures, tables, and charts. All pages must be numbered. Unnecessarily elaborate brochures or presentations beyond what is sufficient to present a complete and effective proposal are not acceptable and will be discarded without review.

4.A.3. Proposal Classification

The Government anticipates that proposals submitted under this BAA will be unclassified.

4.B. Proposal Content Specifics

Each proposal submitted in response to this BAA shall consist of the following:

Volume 1 – Technical & Management Proposal

Section 1 - Cover Sheet & Transmittal Letter
Section 2 – Summary of Proposal
Section 3 – Detailed Proposal
Section 4 – Additional Information

Volume 2 – Cost Proposal

Section 1– Cover Sheet
Section 2 – Detailed Estimated Cost Breakdown

4.B.1. Volume 1, Technical and Management Proposal {Limit of 30 pages}

Volume 1, Technical and Management Proposal, may include an attached bibliography of relevant technical papers or research notes (published and unpublished) which document the technical ideas and approach on which the proposal is based. Copies of not more than three relevant papers can be included with the submission. The submission of other supporting materials along with the proposal is strongly discouraged and will not be considered for review. Except for the cover sheet, transmittal letter, signed Academic Institution Acknowledgement Letter(s) if required, OCI waiver/certification, bibliography, and relevant papers, Volume 1 shall not exceed 30 pages. Any pages exceeding this limit will be removed and not considered during the evaluation process. Full proposals must be accompanied by an official transmittal letter. All full proposals must be written in English.

Section 1: Cover Sheet & Transmittal Letter

A. Cover sheet:
(1) BAA number
(2) Lead organization submitting proposal
(3) Type of business, selected among the following categories: "LARGE BUSINESS", "SMALL DISADVANTAGED BUSINESS", "OTHER SMALL BUSINESS", "HBCU", "MI", "OTHER EDUCATIONAL", OR "OTHER NONPROFIT"
(4) Contractor's reference number (if any)
(5) Other team members (if applicable) and type of business for each
(6) Proposal title
(7) Technical point of contact to include: title, first name, last name, street address, city, state, zip code, telephone, fax (if available), electronic mail (if available)
(8) Administrative point of contact to include: title, first name, last name, street address, city, state, zip code, telephone, fax (if available), electronic mail (if available)
(9) OCI waiver or certification [see Section 3.A.1.] included? Yes/No
(9a) If no, reason for not including?
(10) Are one or more U.S. Academic Organizations part of your team? Yes/No
(10a) If Yes, are you including an Academic Institution Acknowledgement Statement with your proposal for each Academic Organization that is part of your team? Yes/No
(11) Total funds requested from IARPA and the amount of cost share (if any)
(12) Date proposal was submitted.

B. Official Transmittal Letter.

Section 2: Summary of Proposal

Section 2 shall provide an overview of the proposed work as well as introduce associated technical and management issues. This section shall contain a technical description of and technical approach to the research as well as a succinct portrayal of the uniqueness and benefits of the proposed work. It shall make the technical objectives clear and quantifiable and shall provide a project schedule with definite decision points and endpoints. Offerors must address:

A. Innovative claims for the proposed research. This section is the centerpiece of the proposal and should succinctly describe the uniqueness and benefits of the proposed approach relative to the state-of-the-art and alternate technologies and approaches.

B. Summary of the products, transferable technology and deliverables associated with the proposed research results. Measurable deliverables should be defined that show progress toward achieving the stated Program Milestones. Include in this section all proprietary claims to the results, prototypes, intellectual property, or systems supporting and/or necessary for the use of the research, results, and/or prototype. If there are no proprietary claims, this should be stated. Should no proprietary claims be made, Government rights will be unlimited.

C. Schedule and milestones for the proposed research, including overall estimates of cost for each task. Summarize, in table form, the cost, schedule and milestones for the proposed research, including estimates of cost for each deliverable, total cost and company cost share, if applicable. Do not include proprietary information with the milestones.

D. Overview of the technical approach and plan. Technical rationale, technical approach and constructive plan for accomplishing the technical goals that realize the innovative claims and deliverables. (This section will be supplemented with a more detailed plan in Volume 1, Section 3 of the proposal.)

E. Related research. General discussion of other research in this area.

F. Project contributors. Offerors must include a clearly defined organizational chart of all anticipated project participants, their countries of citizenship, and their roles in the project. Accompanying this chart, offerors will provide brief biographical sketches of key personnel and significant contributors and a detailed description of the roles that contributors (including Principal Investigator(s)) will play based on their qualifications and on their level of effort in each year of the Program. Discussion of the teaming strategy among team members shall be included. If the team intends to use consultants, they must be included in the organizational chart as well. Indicate if the person will be an "individual" or "organizational" consultant (that is, will the consultant represent himself/herself or his/her organization). In both cases, the organizational affiliation should be identified. The consultant should make a written commitment to be available to the team; the commitment should be attached to the Cost Volume. (Interested parties are encouraged to leverage personnel that are dedicated to BAA requirements no less than 10% of their time. If any participant is scheduled for less than 10% of his/her time, the proposer will provide a clear and compelling justification as to how benefit can be gained from that person's participation at the specified level of effort.)

A chart, such as the following, is suggested.

Participants	Country of Citizenship	Org	Role	Unique, Relevant Capabilities	Specific Task(s) / Contributions	Time Commitment
John Doe	USA	ABC University	PI/Key Personnel	Programming Languages	Directs Research	25%
John Doe, Jr.	USA	ABC University	Key Personnel	Vulnerability Analysis	Algorithm Design	25%
Jane Doe	England	ABC University	Significant Contributor	And so forth…	And so forth…	50%

Jane Roe	India	ABC University	Contributor			25%
John Doe, III	USA	XYZ Co.	Co-PI/Key Personnel			25%
Wayne Roe	Argentina	XYZ Co.	Significant Contributor			40%
John Doe, IV	USA	XYZ University	Consultant (Individual)			200 hours

Section 3: Detailed Proposal Information

This section of the proposal shall provide the detailed, in-depth discussion of the proposed research. Specific attention must be given to addressing both the risks and payoffs of the proposed research and why it is desirable for IARPA to pursue. This part shall provide:

A. Statement of Work (SOW) - In plain English, clearly define the technical tasks and sub-tasks to be performed, their durations and the dependencies among them. For each task and sub-task, provide:
   - A general description of the objective;
   - A detailed description of the approach to be taken, developed in an orderly progression and in enough detail to establish the feasibility of accomplishing the goals of the task;
   - Identification of the primary organization responsible for task execution (prime, sub-contractor, team member, etc.) by name;
   - The exit criteria for each task/activity, i.e., a product, event or milestone that defines its completion;
   - Definition of all deliverables (e.g., data, reports, software, etc.) to be provided to the Government in support of the proposed research tasks/activities.

   Note: The SOW should be developed so that the Base and Option Periods of the program are separately defined. Do not include any proprietary information in the SOW.

   At the end of this section, provide a Gantt chart, showing all the tasks and sub-tasks on the left with the performance period (in years/quarters) on the right. All milestones should be clearly labeled on the chart.

B. A detailed description of the objectives, scientific relevance, technical approach and expected significance of the work. The key elements of the proposed work should be clearly identified and related to each other. Proposals should clearly detail the technical method(s) and/or approach(es) that will be used to meet or exceed each program milestone and should provide ample justification as to why the proposed method(s)/approach(es) is/are feasible. Any anticipated risks should be described and possible mitigations proposed. General discussion of the problem without specific detail about the technical implementation will result in an unacceptable rating.

C. State-of-the-art. Comparison with other on-going research, highlighting the uniqueness of the proposed effort/approach and differences between the proposed effort and the current state-of-the-art clearly stated. Identify the advantages and disadvantages of the proposed work with respect to potential alternative approaches.

D. Data sources: Identification and description of data sources to be utilized in pursuit of the project research goals. Identify sources of test data and describe test cases planned.

E. Description of the deliverables associated with the proposed research results, enhancing that of Volume 1, Section 2: Summary of Proposal. Deliverables should be defined that show progress toward achieving the stated Program Milestones. Deliverables should be specified at months 6, 12, 16, and 18, for Phase 1, at months 24, 28, and 30, for Phase 2, and at months 36, 42, 46, and 48 for Phase 3. See Section 1.B for more information on Program Milestones. For all software deliverables developed under an agreement or contract, the offeror shall include all executables

and all as delivered version source code produced in the course of software development. Describe any additional software (e.g., open source), systems, or hardware on which the research results/prototype will depend. Describe the proposed approach to intellectual property rights, together with supporting rationale of why this approach offers the best value to the Government. This section should include a list of technical data, computer software or computer software documentation associated with this research effort in which the Government will acquire less than unlimited rights. Should no proprietary claims be made, Government rights will be unlimited. (See also Section 6.B.3, Intellectual Property.)

F. Cost, schedule, milestones. Cost, schedule, and milestones for the proposed research, including estimates of cost for each deliverable delineated by the primes and major sub-contractors, total cost, and company cost share, if any. Where the effort consists of multiple portions that could reasonably be partitioned for purposes of funding, these should be identified as options with separate cost estimates for each. The milestones must not include proprietary information.

G. Offeror's previous accomplishments. Discuss previous accomplishments and work in this or closely related research areas and how these will contribute to and influence the current work.

H. Facilities. Describe the facilities that will be used for the proposed effort, including computational and experimental resources.

I. Detailed Management Plan. The Management Plan should identify both the organizations and the individuals within those organizations that make up the team and delineate the expected duties, relevant capabilities and task responsibilities of team members and expected relationships among team members. Expected levels of effort (percentage time or fraction of an FTE) for all key personnel and significant contributors should be clearly noted. A description of the technical, administrative and business structure of the team and the internal communications plan should be included. Project/function/sub-contractor relationships (including formal teaming agreements), Government research interfaces, and planning, scheduling, and control practices should be described. The team leadership structure should be clearly defined. Provide a brief biography of the key personnel (including alternates, if desired) who will be involved in the research along with the amount of effort to be expended by each person during the year. Participation by key personnel and significant contributors is expected to be at least 10% of their time. A compelling explanation of any variation from this figure is required.

J. Resource Share. Include the type of support, if any, the offeror might request from the Government, such as facilities, equipment or materials, or any such resources the offeror is willing to provide at no additional cost to the Government to support the research effort. Cost sharing is not required from offerors and is not an evaluation criterion, but is encouraged where there is a reasonable probability of a potential commercial application related to the proposed research and development effort.

K. The names of other federal, state or local agencies or other parties receiving the proposal and/or funding the proposed effort. If none, so state.

Section 4: Additional Information

A brief bibliography of relevant technical papers and research notes (published and unpublished) which document the technical ideas on which the proposal is based. Copies of not more than three (3) relevant papers may be included in the submission. This information does not contribute to the page count of Volume 1.

4.B.2. Volume 2: Cost Proposal {No Page Limit}

Section 1: Cover Sheet

(1) BAA number;

(2) Lead organization submitting proposal
(3) Type of business, selected among the following categories: "LARGE BUSINESS", "SMALL DISADVANTAGED BUSINESS", "OTHER SMALL BUSINESS", "HBCU", "MI", "OTHER EDUCATIONAL", OR "OTHER NONPROFIT"
(4) Contractor's reference number (if any)
(5) Other team members (if applicable) and type of business for each
(6) Proposal title
(7) Technical point of contact to include: title, first name, last name, street address, city, state, zip code, telephone, fax (if available), electronic mail (if available)
(8) Administrative point of contact to include: title, first name, last name, street address, city, state, zip code, telephone, fax (if available), and electronic mail (if available)
(9) Award instrument requested: cost-plus-fixed-fee (CPFF), cost-contract—no fee, cost sharing contract – no fee, grant, cooperative agreement, other transaction or other type of procurement contract (specify)
(10) Place(s) and period(s) of performance
(11) Total proposed cost separated by basic award and option(s) (if any)
(12) Name, address, telephone number of the offeror's Defense Contract Management Agency (DCMA) administration office or equivalent cognizant contract administration entity, if known
(13) Name, address, telephone number of the offeror's Defense Contract Audit Agency (DCAA) audit office or equivalent cognizant contract audit entity, if known
(14) Date proposal was prepared
(15) DUNS number
(16) TIN number
(17) Cage Code
(18) Proposal validity period [minimum of 90 days]

[NOTE: See Appendix B for Cover Sheet Template]

Section 2: Detailed Estimated Cost Breakdown

(1) Total cost broken down by major cost items (direct labor, including labor categories; sub-contracts; materials; other direct costs, overhead charges, etc.) and further broken down by major task and phase
(2) Major program tasks by fiscal year
(3) An itemization of major subcontracts and equipment purchases

(4) An itemization of any information technology (IT[7]) purchase
(5) A summary of projected funding requirements by month
(6) The source, nature and amount of any industry cost-sharing
(7) Identification of pricing assumptions of which may require incorporation into the resulting award instrument (e.g., use of Government Furnished Property/Facilities/Information, access to Government Subject Matter Expert/s, etc.).

The prime contractor is responsible for compiling and providing all subcontractor proposals for the Procuring Contracting Officer (PCO). Subcontractor proposals should include Interdivisional Work Transfer Agreements (ITWA) or similar arrangements. Where the effort consists of multiple portions which could reasonably be partitioned for purposes of funding, these should be identified as options with separate cost estimates for each. NOTE: For IT and equipment purchases, include a letter stating why the offeror cannot provide the requested resources from its own funding.

Supporting cost and pricing information must be provided in sufficient detail to substantiate the summary cost estimates in Volume 1 above. Include a description of the method used to estimate costs and supporting documentation. Note: "cost or pricing data" shall be required if the offeror is seeking a procurement contract award of $650,000 or greater unless the offeror requests an exception from the requirement to submit cost or pricing data. Cost or pricing are not required if the offeror proposes an award instrument other than a procurement contract (e.g., a grant, cooperative agreement, or other transaction). However, such data may be required prior to award if the offeror's proposal is selected for negotiations and the Government determines that a procurement contract is the appropriate award instrument. All proprietary subcontractor proposal documentation, prepared at the same level of detail as that required of the prime, shall be made immediately available to the Government, upon request, under separate cover (i.e., mail, electronic/email, etc.), either by the offeror or by the subcontractor organization.

All offerors requesting an other transaction award instrument must include a detailed list of payment milestones. Each such payment milestone must include the following: milestone description, exit criteria, due date, milestone payment amount (to include, if cost share is proposed, contractor and government share amounts). It is noted that, at a minimum, such payable milestones should relate directly to accomplishment of technical milestones and metrics as defined in the offeror'sproposal. Agreement type, fixed price or expenditure based, will be subject to negotiation by the Government; however, it is noted that the Government prefers use of fixed price payable milestones to the maximum extent possible. Do not include proprietary data.

Consultant letter(s) of commitment should be attached to the Cost Volume and estimated costs should be included in the cost estimates.

[7]IT is defined as "any equipment, or interconnected system(s) or subsystem(s) of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. (a) For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency which – (1) Requires the use of such equipment; or (2) Requires the use, to a significant extent, or such equipment in the performance of a service or the furnishing of a product. (b) The term "information technology" includes computers, ancillary, software, firmware and similar procedures, services (including support services), and related resources. (c) The term "information technology" does not include – (1) Any equipment that is acquired by a contractor incidental to a contract; or (2) Any equipment that contains imbedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment, such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, is not information technology."

4.C. Submission Details

4.C.1. Due Dates

Proposals must be submitted at or before 5:00 p.m. local time on November 2, 2009, in order to be considered during the initial round of selections.

4.C.2. Proposal Delivery

The full proposal (one original hard copy with original signatures; one hard copy with original or copied signatures; and 1 electronic copy with Volume 1, Volume 2 and any permitted, additional information (.pdf format preferred) on a CD-ROM), and any abstract must be delivered to:

ODNI/IARPA
Attention: Dr. Carl Landwehr
Gate 5
1000 Colonial Farm Road
McLean, VA 22101

IMPORTANT: Deliveries must be made using one of the following commercial delivery services: UPS, FedEx or DHL. Failure to use one of these methods may jeopardize or delay delivery of proposals. Note that under certain "same day delivery" options, UPS, FedEx and DHL may subcontract out their services to local delivery companies. These smaller local delivery companies will not be allowed access to this address to make deliveries. For this reason and other unforeseen situations, offerors should track their submission to ensure final delivery. Deliveries by hand, e-mail or fax will not be accepted.

Offerors must ensure the timely delivery of their proposals. The mail facility closes at 5 p.m. local time; delivery cannot take place after this time until the following day. IARPA will generally acknowledge receipt of complete submissions via e-mail within 24-48 hours and assign control numbers that should be used in all further correspondence regarding proposals. To be certain of delivery, however, it is suggested that a tracking number be obtained from the carrier.

Offerors are required to submit proposals by the time and date specified in the BAA in order to be considered during the initial round of selections. IARPA may evaluate proposals received after this date for a period up to one year from the date of initial posting on FedBizOpps. Selection remains contingent on availability of funds.

Failure to comply with the submission procedures may result in the submission not being evaluated.

SECTION 5: APPLICATION REVIEW INFORMATION

5.A. Evaluation Criteria

The criteria to be used to evaluate and select proposals for this Program BAA are described in the following paragraphs. Because there is no common statement of work, each proposal will be evaluated on its own merits and its relevance to the Program goals rather than against other proposals responding to this BAA. Specifics about the evaluation criteria are provided below, in descending order of importance.

5.A.1. Overall Scientific and Technical Merit

Overall scientific and technical merit of the proposal is substantiated, including unique and innovative methods, approaches, and/or concepts. The offeror clearly articulates an understanding of the problem to be solved. The technical approach is credible, and includes a clear assessment of primary risks and a means to address them. The offeror can expect the selection process to include an assessment of the proposal against the state-of-the-art.

5.A.2. Effectiveness of Proposed Work Plan

The feasibility and likelihood that the proposed approach for satisfying the Program's milestones and metrics are explicitly described and clearly substantiated along with risk mitigation strategies for achieving stated milestones and metrics. The proposal reflects a mature and quantitative understanding of the Program milestones and metrics, and the statistical confidence with which they may be measured. The offeror may also propose additional milestones and metrics as needed. Any such milestones and metrics are clear and well-defined, with a logical connection to enabling offeror decisions and/or Government decisions. The schedule to achieve the milestones is realistic and reasonable.

Exploiting the synergy of integrating new methods for analysis, confinement and diversification is especially important. The offeror's approach should lead to a single comprehensive solution that takes advantage of the complementary aspects of these three methods.

The role and relationships of prime and sub-contractors is clearly delineated with all participants fully documented. Work plans demonstrate the ability to provide full Government visibility into and interaction with key technical activities and personnel; and a single point of responsibility for contract performance. Work plans must also demonstrate that key personnel have sufficient time committed to the Program to accomplish their described Program roles.

The requirement for and the anticipated use or integration of Government Furnished Property (GFP) including all equipment, facilities, information, etc., is fully described including dates when such GFP, GFE (Government Furnished Equipment), GFI (Government Furnished Information) or other similar Government-provided resources will be required.

The offeror's proposed intellectual property and data rights are consistent with the Government's need to be able to communicate Program information across Government organizations and to support transition of the Program results to Intelligence Community users at a reasonable cost.

5.A.3. Contribution and Relevance to the IARPA Mission and STONESOUP Goals

The proposed solution meets the letter and intent of the stated program goals and all elements within the proposal exhibit a comprehensive understanding of the problem. The offeror clearly addresses how the proposed effort will meet and progressively demonstrate STONESOUP Program goals. The offeror describes how the proposed solution contributes to IARPA's mission to invest in high-risk/high-payoff research that can provide the U.S. with an overwhelming intelligence advantage over its future adversaries. The proposed approach to intellectual property rights offers the best value to the Government.

5.A.4. Relevant Experience and Expertise

The offeror's capabilities, related experience, facilities, techniques, or unique combination of these which are integral factors for achieving the proposal's objectives will be evaluated, as well as qualifications,

capabilities, and experience of the proposed principal investigator, team leader, and key personnel critical in achieving the proposal objectives. Time commitments of key personnel must be sufficient for their proposed responsibilities in the effort.

Experience and expertise in all three methods, i.e., analysis, confinement and diversification is especially important. Offerors should ensure that their team includes personnel skilled in all three methods as appropriate.

5.A.5. Cost Realism

The proposed costs are reasonable and realistic for the work proposed. Estimates are "realistic" when they are neither excessive nor insufficient for the effort to be accomplished. The proposal documents all anticipated costs including those of associate, participating organizations. The proposal demonstrates that the respondent has fully analyzed budget requirements and addressed resulting cost risks. Other sponsors who have funded or are funding this offeror for the same or similar efforts are identified. The Government shall evaluate how well all cost data are traceable and reconcilable.

IARPA recognizes that undue emphasis on cost may motivate Offerors to offer low-risk ideas with minimum uncertainty and to staff the effort with junior personnel in order to be in a more competitive posture. IARPA discourages such cost strategies. Cost reduction approaches that will be received favorably include innovative management concepts that maximize direct funding for technology and limit diversion of funds into overhead.

After selection and before award, the Contracting Officer will negotiate cost/price reasonableness.

5.B. Review and Selection Process

It is the policy of IARPA to ensure impartial, equitable, comprehensive proposal evaluations and to select the source (or sources) whose offer meets the Government's technical, policy and programmatic goals. In order to provide the desired evaluation, qualified Government personnel will conduct reviews and (if necessary) convene panels of experts in the appropriate areas.

Proposals will only be evaluated against the criteria described under Section 5.A above, and will not be evaluated against other proposals since they are not submitted in accordance with a common work statement. For evaluation purposes, a proposal is the document described in Section 4. Other supporting or background materials submitted with the proposal will be considered for the reviewer's convenience only and not considered as part of the proposal.

As noted above, the Government intends to use employees of Omen, LLC, Teknoworks, Inc., and The University Of Maryland, College Park to provide expert advice regarding portions of the proposals submitted to the Government. Booz Allen Hamilton will also provide logistical support in carrying out the evaluation process. These personnel will have signed and be subject to the terms and conditions of non-disclosure agreements. By submission of its proposal, an offeror agrees that its proposal information may be disclosed to employees of these organizations for the limited purpose stated above. If you do not send notice of objection to this arrangement, the Government will assume your consent to the use of contractor support personnel in assisting the review of your submittal(s) under this BAA. Only Government personnel will make evaluations and award determinations under this BAA.

5.C. Proposal Retention

It is the policy of IARPA to treat all proposals as competitive information and to disclose their contents only for the purpose of evaluation. Proposals will not be returned. Upon completion of the source selection process, the original of each proposal received will be retained at IARPA and all other non-required copies will be destroyed. A certification of destruction may be requested, provided that the formal request is sent to IARPA via e-mail within 5 days after notification of proposal results.

SECTION 6: AWARD ADMINISTRATION INFORMATION

6.A. Award Notices

As soon as the evaluations are complete, the offeror will be notified by the Program Manager that 1) the proposal has been selected for funding, pending contract negotiations or 2) the proposal has not been selected for funding. The Government Contracting Officer will send similar notification to the Contracting Office/Administrative Point of Contact of the lead organization.

6.B. Administrative and National Policy Requirements

6.B.1. Security

The Government anticipates that abstracts and proposals submitted under this BAA will be unclassified.

6.B.2 Proprietary Data

It is the policy of IARPA to treat all proposals as competitive information, and to disclose their contents only for the purpose of evaluation.

All proposals containing proprietary data should have the cover page and each page containing proprietary data clearly marked as containing proprietary data. It is the offeror's responsibility to clearly define to the Government what is considered proprietary data.

6.B.3. Intellectual Property

6.B.3.a. Procurement Contract Offerors

6.B.3.a.1. Noncommercial Items (Technical Data and Computer Software)

Offerors responding to this BAA requesting a procurement contract to be issued under the FAR shall identify all noncommercial technical data and noncommercial computer software that it plans to generate, develop and/or deliver under any proposed award instrument in which the Government will acquire less than unlimited rights and to assert specific restrictions on those deliverables. In the event that offerors do not submit such information, the Government will assume that it automatically has "unlimited rights" to all noncommercial technical data and noncommercial computer software generated, developed, and/or delivered under any award instrument, unless it is substantiated that development of the noncommercial technical data and noncommercial computer software occurred with mixed funding. If mixed funding is anticipated in the development of noncommercial technical data and noncommercial computer software generated, developed and/or delivered under any award instrument, then offerors should identify the data and software in question as subject to Government Purpose Rights (GPR).[8] The Government will

[8] "Government purpose rights" means the rights to use, modify, reproduce, release, perform, display, or disclose technical data and computer software within the Government without restriction; and to release or disclose technical

automatically assume that any such GPR restriction is limited to a period of five (5) years, at which time the Government will acquire "unlimited rights" unless the parties agree otherwise. Offerors are advised that the Government will use this information during the source selection evaluation process to evaluate the impact of any identified restrictions and may request additional information from the offeror, as may be necessary, to evaluate the offeror's assertions. If no restrictions are intended, then the offeror should state "NONE."

A sample list for complying with this request is as follows:

NONCOMMERCIAL ITEMS			
Technical Data, Computer Software To be Furnished With Restrictions	Basis for Assertion	Asserted Rights Category	Name of Person Asserting Restrictions
(LIST)	(LIST)	(LIST)	(LIST)

6.B.3.a.2. Commercial Items (Technical Data and Computer Software)

Offerors responding to this BAA requesting a procurement contract to be issued under the FAR shall identify all commercial technical data and commercial computer software that may be embedded in any noncommercial deliverables contemplated under the research effort, along with any applicable restrictions on the Government's use of such commercial technical data and/or commercial computer software. In the event that offerors do not submit the list, the Government will assume that there are no restrictions on the Government's use of such commercial items. The Government may use the list during the source selection evaluation process to evaluate the impact of any identified restrictions and may request additional information from the offeror, as may be necessary, to evaluate the offeror's assertions. If no restrictions are intended, then the offeror should state "NONE."

A sample list for complying with this request is as follows:

COMMERCIAL ITEMS			
Technical Data, Computer Software To be Furnished With Restrictions	Basis for Assertion	Asserted Rights Category	Name of Person Asserting Restrictions
(LIST)	(LIST)	(LIST)	(LIST)

6.B.3.a.3. Non-Procurement Contract Offerors – Noncommercial and Commercial Items (Technical Data and Computer Software)

Offerors responding to this BAA requesting a grant, cooperative agreement, technology investment agreement, or other transaction shall follow the applicable rules and regulations governing these various award instruments, but in all cases should appropriately identify any potential restrictions on the Government's use of any Intellectual Property contemplated under those award instruments in question. This includes both Noncommercial Items and Commercial Items. Offerors may use a format similar to

---

data and computer software outside the Government and authorize persons to whom release or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose that data or software for any United States Government purpose. United States Government purposes include any activity in which the United States Government is a party, including cooperative agreements with international or multi-national defense organizations, or sales or transfers by the United States Government to foreign governments or international organizations. Government purposes include competitive procurement, but do not include the rights to use, modify, reproduce, release, perform, display, or disclose technical data or computer software for commercial purposes or authorize others to do so.

that described in the previous sections. The Government may use the list during the source selection evaluation process to evaluate the impact of any identified restrictions, and may request additional information from the offeror, as may be necessary, to evaluate the offeror'sassertions. If no restrictions are intended, then the offeror should state "NONE."

6.B.3.b. All Offerors – Patents

Include documentation proving ownership of or possession of appropriate licensing rights to all patented inventions (or inventions for which a patent application has been filed) that will be utilized under the proposal for the IARPA program. If a patent application has been filed for an invention that the proposal utilizes, but the application has not yet been made publicly available and contains proprietary information, the offeror may provide only the patent number, inventor name(s), assignee names (if any), filing date, filing date of any related provisional application, and a summary of the patent title, together with either: 1) a representation that the offeror owns the invention, or 2) proof of possession of appropriate licensing rights in the invention.

6.B.3.c. All Offerors – Intellectual Property Representations

All offerors shall provide a good faith representation that you either own or possess appropriate licensing rights to all other intellectual property that will be utilized under your proposal for the IARPA program. Additionally, offerors shall provide a short summary for each item asserted with less than unlimited rights that describes the nature of the restriction and the intended use of the intellectual property in the conduct of the proposed research.

6.B.4. Meeting and Travel Requirements

Performers are expected to assume responsibility for administration of their projects and to comply with contractual and Program requirements for reporting, attendance at Program workshops and availability for site visits.

6.B.4.a. Program Reviews

The STONESOUP Program intends to hold a Program-Level Kickoff Meeting in the first month of each program phase and then hold Program-Level Reviews in accordance with the schedule in Table 4. These 2-3 day Reviews will focus on technical aspects of the Program and on facilitating open technical exchanges, interaction and sharing among the various Program participants. Program participants will be expected to present the technical status and progress of their projects as well as to demonstrate their technical capabilities to other participants and invited guests at these events. For costing purposes, the offeror should expect Workshop locations to alternate between the Washington, D.C., area and outside the Washington, D.C., area.

6.B.4.b. Site Visits

Site visits by the Contracting Officer Representative and the STONESOUP Program Management staff will generally take place twice yearly during the life of the Program and will occur during the period between Program-level Workshops. These visits will occur at the Contractor's facility. Reports on technical progress, details of successes and issues, contributions to the Program goals and technology demonstrations will be expected at such visits.

6.B.5. Human Use

All research involving human subjects, to include use of human biological specimens and human data, selected for funding must comply with the federal regulations for human subject protection, namely 45 CFR Part 46, *Protection of Human Subjects* (http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.htm) and 32 CFR Part 219 *Protection of Human Subjects* (http://www.dtic.mil/biosys/downloads/32cfr219.pdf).

Institutions awarded funding for research involving human subjects must provide documentation of a current Assurance of Compliance with Federal regulations for human subject protection, for example a Department of Health and Human Services, Office of Human Research Protection Federal Wide Assurance (http://www.hhs.gov/ohrp). All institutions engaged in human subject research, to include sub-contractors, must also have a valid Assurance.

For all proposed research that will involve human subjects in the first year of the program, the institution must provide evidence of or a plan for review by an Institutional Review Board (IRB) on final proposal submission to IARPA. The IRB conducting the review must be the IRB identified on the institution's Assurance. The protocol, separate from the proposal, must include a detailed description of the research plan, study population, risks and benefits of study participation, recruitment and consent process, data collection, and data analysis. Consult the designated IRB for guidance on writing the protocol. The informed consent document must comply with federal regulations (45 CFR Part 46 and 32 CFR 219.116).

The STONESOUP Program plans to use a DoD Contracting Agent. In addition to a local IRB approval, a headquarters-level human-subject regulatory review and approval is required for all research conducted or supported by the DoD. The DoD office responsible for managing the award can provide guidance and information about their component's headquarters-level review process. Note that confirmation of a current Assurance and appropriate human-subject-protection training is required before headquarters-level approval can be issued.

The amount of time required to complete the IRB review/approval process may vary depending on the complexity of the research and/or the level of risk to study participants. Ample time should be allotted to complete the approval process. The IRB approval process can last between one to three months, followed by a DoD review that could last between three to six months. No IARPA funding can be used towards human-subject research until ALL approvals are granted.

In limited instances, human subject research may be exempt from Federal regulations for human subject protection, for example, under Department of Health and Human Services, 45 CFR 46.101(b). Offerors claiming that their research falls within an exemption from Federal regulations for human subject protection must provide written documentation with their proposal that cites the specific applicable exemption and explains clearly how their proposed research fits within that exemption.

6.B.6. Publication Approval

It is anticipated that research funded under this Program will be unclassified contracted fundamental research that will not require a pre-publication review. However, performers should note that pre-publication approval of certain information may be required if it is determined that its release may result in the disclosure of sensitive intelligence information. A courtesy soft copy of any work submitted for publication should be provided to the IARPA Program Manager and the Contracting Officer Representative (COR).

6.B.7. Export Control

(1) The offeror shall comply with all U.S. export control laws and regulations, including the International Traffic in Arms Regulations (ITAR), 22 CFR Parts 120 through 130, and the Export Administration Regulations (EAR), 15 CFR Parts 730 through 799, in the performance of this contract. In the absence of available license exemptions/exceptions, the offeror shall be responsible for obtaining the appropriate licenses or other approvals, if required, for exports of (including deemed exports) hardware, technical data, and software, or for the provision of technical assistance.

(2) The offeror shall be responsible for obtaining export licenses, if required, before utilizing foreign persons in the performance of this contract, including instances where the work is to be performed on-site at any Government installation (whether in or outside the United States), where the foreign person will have access to export-controlled technologies, including technical data or software.

(3) The offeror shall be responsible for all regulatory record keeping requirements associated with the use of licenses and license exemptions/exceptions.

(4) The offeror shall be responsible for ensuring that the provisions of this clause apply to its sub-contractors**.**

(5) The offerorwill certify knowledge of and intended adherence to these requirements in the representations and certifications of the contract.

6.B.8. Subcontracting

It is the policy of the Government to enable small business and small disadvantaged business concerns to be considered fairly as sub-contractors to contractors performing work or rendering services as prime contractors or sub-contractors under Government contracts and to assure that prime contractors and sub-contractors carry out this policy. Each offeror that submits a proposal that includes sub-contractors; is selected for funding (pending negotiations); and has proposed a funding level above the maximum cited in the FAR, may be asked to submit a sub-contracting plan before award, in accordance with FAR 19.702(a) (1) and (2). The plan format is outlined in FAR 19.704.

6.B.9. Reporting

Fiscal and management responsibility are important to the STONESOUP Program. Although the number and types of reports will be specified in the award document, all performers will, at a minimum, provide the Contracting Office, Contracting Officer Representative and the STONESOUP Program Manager with monthly technical reports and monthly financial reports. The reports shall be prepared and submitted in accordance with the procedures contained in the award document and mutually agreed upon before award. Technical reports will describe technical highlights and accomplishments, priorities and plans, issues and concerns; will provide evaluation results; and will detail future plans. Financial reports will present an on-going financial profile of the project, including total project funding, funds invoiced, funds received, funds expended during the preceding month and planned expenditures over the remaining period. Additional reports and briefing material may also be required, as appropriate, to document progress in accomplishing program metrics.

Performers will prepare a final report of their work at the conclusion of the performance period of the award (even if the research may continue under a follow-on vehicle). The final report will be delivered to the Contracting Agent, Contracting Officer Representative and the STONESOUP Program Manager. The report will include:

- Problem definition
- Findings and approach
- System design and solution
- Possible generalization(s)
- Anticipated path ahead
- Lessons learned
- Suggestions for future research

6.B.10. Central Contractor Registration (CCR)

Selected offerors not already registered in the Central Contractor Registry (CCR) may be required to register in CCR prior to any award under this BAA. Information on CCR registration is available at http://www.ccr.gov**.**

6.B.11. Representations and Certifications

Prospective offerors may be required to complete electronic representations and certifications at http://orca.bpn.gov. Successful offerors will be required to complete additional representations and certifications prior to award.

6.B.11.a. Certification for Grant Awards

The certification at Appendix A to 32 CFR Part 28 regarding lobbying is the only certification required at the time of proposal submission for a grant award. The certification is as follows:

"By signing and submitting a proposal that may result in the award of a grant exceeding $100,000, the prospective awardee is certifying, to the best of his or her knowledge and belief, that:

(a) No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

(b) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

(c) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty or not less than $10,000 and not more than $100,000 for each such failure."

6.B.11.b. Certification for Contract Awards

Certifications and representations shall be completed by successful offerors prior to award. Federal Acquisition Regulation (FAR) Online Representations and Certifications Application (ORCA) is at website http://orca.bpn.gov. Defense FAR Supplement and contract specific certification packages will be provided to the contractor for completion prior to award.

6.B.12. Wide Area Work Flow (WAWF)

Any contract award resulting from this solicitation will contain the clause at DFARS 252.232-7003, Electronic Submission of Payment Requests, which requires electronic submission of all payment requests. The clause cites three possible electronic formats through which to submit electronic payment requests. Pursuant to that clause, the Department of Defense is adopting Wide Area Work Flow-Receipt and Acceptance (WAWF-RA). Any contract resulting from this solicitation will establish a requirement to use WAWF-RA for invoicing and receipt/acceptance, and provide coding instructions applicable to this contract. Contractors are encouraged to take advantage of available training (both web-based and through your local DCMA office), and to register in the WAWF-RA system. Information regarding WAWF-RA, including the web-based training and registration, can be found at https://wawf.eb.mil. Note: This WAWF-RA requirement does not apply to Universities that are audited by an agency other than DCAA.

SECTION 7: AGENCY CONTACTS

Administrative, technical or contractual questions concerning this BAA should be sent via e-mail todni-iarpa-baa-09-08@ugov.gov. If e-mail is not available, fax questions to 301-226-9137, Attention: IARPA-BAA-09-08.All requests must include the name, email address (if available), and phone number of a point of contact for the requested information. Do not send questions with proprietary content. IARPA will accept questions about the BAA until its closing. A consolidated Question and Answer response will be periodically posted on the IARPA website (www.IARPA.gov); no answers will go directly to the submitter.

Points of Contact:

The technical POC for this effort is

Dr. Carl Landwehr IARPA, Safe and Secure Operations Office
ATTN: IARPA-BAA-09-08
Office of the Director of National Intelligence
Intelligence Advanced Research Projects Activity (IARPA)
Washington, DC 20511
Fax: (301) 226-9137
E-mail:dni-iarpa-baa-09-08@ugov.gov

All emails must have the BAA number (IARPA-BAA-09-08) in the Subject Line.

APPENDIX A

Academic Institution Acknowledgement Letter Template

IARPA Broad Agency Announcement

IARPA-BAA-09-08

-- Please Place on Official Letterhead --

<insert date>

To: Mr. Thomas Kelso
Chief Acquisition Officer
ODNI/IARPA
Office of the Director of National Intelligence
Washington, D.C. 20511

Subject: Academic Institution Acknowledgement Letter

Reference: Executive Order 12333, As Amended, Para 2.7

This letter is to acknowledge that the undersigned is the responsible official of <insert name of the academic institution>, authorized to approve the contractual relationship in support of the Office of the Director of National Intelligence's Intelligence Advanced Research Projects Activity and this academic institution.

The undersigned further acknowledges that he/she is aware of the Intelligence Advanced Research Projects Activity's proposed contractual relationship with <insert name of institution> through <insert solicitation #> and is hereby approved by the undersigned official, serving as the president, vice-president, chancellor, vice-chancellor, or provost of the institution.

_____

<Name> Date
<Position>

Copy Furnished:
Mr. John Turnicky
Chief, ODNI Contracts
Office of the Director of National Intelligence
Washington, DC 20511

APPENDIX B

SAMPLE COVER SHEET

for

VOLUME 1: Technical/Management Details

BROAD AGENCY ANNOUNCEMENT (BAA)

Securely Taking on New Executable Software of Uncertain Provenance (STONESOUP) Program

IARPA-BAA-09-08

(1) BAA Number	
(2) Lead Organization Submitting Proposal	
(3) Type of Business, Selected Among the Following Categories: "Large Business", "Small Disadvantaged Business", "Other Small Business", "HBCU", "MI", "Other Educational", or "Other Nonprofit"	
(4) Contractor's Reference Number (if any)	
(5) Other Team Members (if applicable) and Type of Business for Each	
(6) Proposal Title	
(7) Technical Point of Contact to Include: Title, First Name, Last Name, Street Address, City, State, Zip Code, Telephone, Fax (if available), Electronic Mail (if available)	
(8) Administrative Point of Contact to Include: Title, First Name, Last Name, Street Address, City, State, Zip Code, Telephone, Fax (if available), Electronic Mail (if available)	
(9) OCI Waiver or Certification [see Section 3.A.1] Included?	Yes/No
(9a) If No, reason for not including?	
(10) Are one or more U.S. Academic Organizations part of your team?	Yes/No
(10a) If Yes, are you including an Academic Institution Acknowledgement Statement with your proposal for each Academic Organization that is part of your team?	Yes/No
(11) Total Funds Requested from IARPA and the Amount of Cost Share (if any)	$
(12) Date Proposal as Submitted.	

APPENDIX C

SAMPLE COVER SHEET

for

VOLUME 2: Cost Proposal

BROAD AGENCY ANNOUNCEMENT (BAA)

Securely Taking on New Executable Software of Uncertain Provenance (STONESOUP) Program

IARPA-BAA-09-08

(1) BAA Number	
(2) Lead organization submitting proposal	
(3) Type of Business, Selected Among the Following Categories: “Large Business”, “Small Disadvantaged Business”, “Other Small Business”, “HBCU”, “MI”, “Other Educational”, or “Other Nonprofit”	
(4) Contractor’s Reference Number (if any)	
(5) Other Team Members (if applicable) and Type of Business for Each	
(6) Proposal Title	
(7) Technical Point of Contact to Include: Title, First Name, Last Name, Street Address, City, State, Zip Code, Telephone, Fax (if available), Electronic Mail (if available)	
(8) Administrative Point of Contact to Include: Title, First Name, Last Name, Street Address, City, State, Zip Code, Telephone, Fax (if available), Electronic Mail (if available)	
(9) Award Instrument Requested: Cost-Plus-Fixed-Fee (CPFF), Cost-Contract—No Fee, Cost Sharing Contract – No Fee, Grant, Cooperative Agreement or Other Type of Procurement Contract (specify)	
(10) Place(s) and Period(s) of Performance	
(11) Total Proposed Cost Separated by Basic Award and Option(s) (if any)	
(12) Name, Address, Telephone Number of the Offeror’s Defense Contract Management Agency (DCMA) Administration Office or Equivalent Cognizant Contract Administration Entity, if Known	
(13) Name, Address, Telephone Number of the Offeror’s Defense Contract Audit Agency (DCAA) Audit Office or Equivalent Cognizant Contract Audit Entity, if Known	
(14) Date Proposal was Prepared	
(15) DUNS Number	
(16) TIN Number	
(17) Cage Code	
(18) Proposal Validity Period [minimum of 90 days]	