

Computer Science Department, Carnegie-Mellon University, Pittsburgh, PA

9/1968–7/1977

- ◆ Ph.D dissertation: Segmentation and Labeling of Speech, a Comparative Performance Evaluation
- ◆ Developed the signal-to-symbol level components of CMU's Hearsay II speech understanding system, supported by DARPA's SUS program in the 1970's.

Jonathan Herr

Software Engineer

Summary of Qualifications

- ◆ Has 10 years experience working on all aspects of the full software development life cycle across a variety of communities.
- ◆ Has 7 years of experience with Java programming language including work on SOA architectures, J2EE solutions, and a variety of client and server libraries.
- ◆ Developed the common evaluation framework used by the DARPA Machine Reading program

Education

- ◆ MS, Computer Science, The Johns Hopkins University, 2007
- ◆ BBA, Computer Information Systems, James Madison University, 1999

Clearance: TS/SCI with Full Scope Polygraph—Active

Work in Related Research Areas and Previous Accomplishments

Science Applications International Corporation, Senior Software Engineer

5/2008–Present

- ◆ Leads software development efforts which support evaluation of intelligent systems.
- ◆ Supports experimentation by building test harnesses which measure system performance.
- ◆ Supports classified projects with Java development and secure communications protocols such as mutually authenticated SSL transactions.

Lockheed Martin Corporation, Software Engineer

5/1999–5/2008

- ◆ Led design and development of a layer for communication between .Net and Java applications using Windows Communications Foundation and C# in Microsoft .Net 3.0.
- ◆ Designed and developed a reporting tool for a 24 hour operations center which displayed live views of incoming data over the web using AJAX and a SOA architecture.
- ◆ Developed ETL component of a large data warehousing project involving terabytes of data being loaded into a MS SQL Server farm.

2.10 Project Management and Interaction Plan

2.10.1 Team Composition

The composition of the SAIC team addresses both the scientific design of evaluations that provide meaningful results, and the engineering needed to build the supporting tools and processes. Prior experience has shown that SAIC, as the evaluator, is the natural facilitator for and has successfully created a common understanding among and between the algorithm teams, as well as with the data collection effort. Our organization reflects this by identifying leads for the critical infrastructure portions of the overall program task, as described in **figure 2.10-1**. SAIC's Principle Investigator (PI) Rich LaValley, supported by an experienced team, will provide the leadership and technical skills needed to execute all parts of the proposed evaluation task. Matt Reardon, Program Manager (PM), will support the program execution and collaboration across Technical Area 1 and 2 performers. SAIC has also arranged to place Dr. Paul Cohen under a consulting agreement to provide expert technical guidance on the conduct of the evaluation.

The Data Preparation activity is called out to address the need for communication and coordination with the team selected to perform the Data Collection task, ensuring the right distribution and composition of the speech samples

provided for training and evaluation by the algorithm development teams. This activity will be heaviest in the initial 6 months of the program.

Under the Experimentation activity, analysts experienced in the real-world applications for large collections of speech data will design experiment-based evaluations that produce useful results. Experiment design will guide data set design, evaluation scenario planning, and analysis and presentation of results to the government for both the unclassified and classified evaluations. The focus on scientific, statistically valid, measurable metrics and experimentation supported by automated tools and processes for analysis, feedback, and recommendations will provide the government with the best value from our evaluation team.

The Framework Development resources proposed for this effort will define the requirements and implement the systems to execute evaluations over the large set of audio data collected, over several different speech processing systems, and operating within both an unclassified and classified environment. Engineers experienced with the DARPA Machine Reading evaluation software framework are proposed for this effort, to leverage the existing software assets as extended to meet the anticipated needs of the algorithm development systems. These

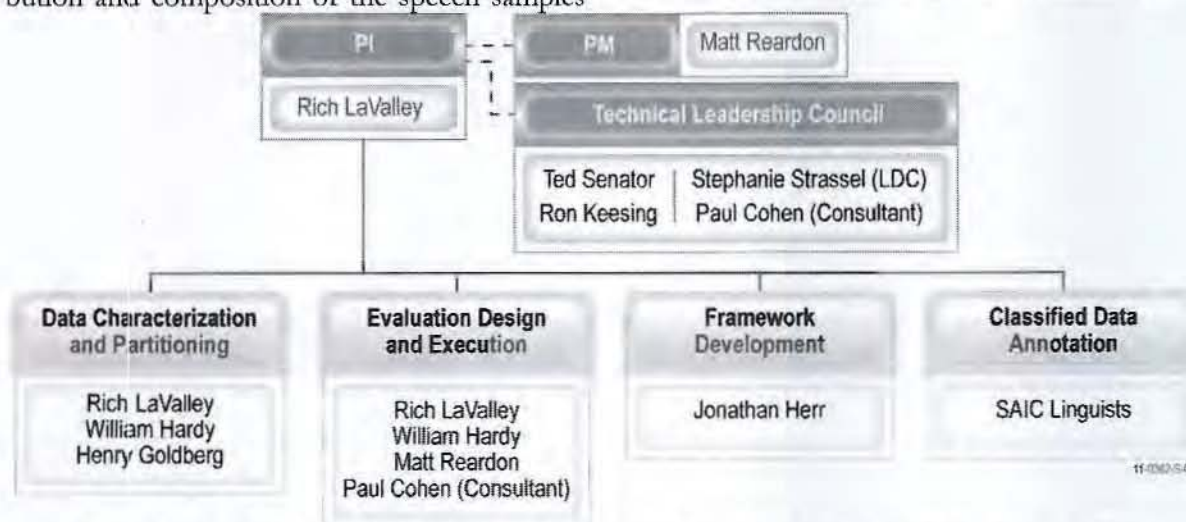


Figure 2.10-1. SAIC's Evaluation Team Collaborate to Bring Science and Engineering to the Evaluation Plan

resources are expected to be utilized in a phased approach to development - heavier in the first 6 months of each yearly phase, preparing the evaluation system to interact with the newest technological advances of the speech processing systems under development, then active at each interim evaluation point to provide feedback and revise code.

The Classified Data Annotation activity will be lead by SAIC linguists, applying common annotation data annotation tools and processes utilized by the Technical Area 2 performer. Level of effort is estimated based on the size of the anticipated data set.

Further, the PM and PI will be supported by a Technical Leadership Council (TLC) consisting of Ted Senator and Ron Keesing from SAIC, and Dr. Paul Cohen from the University of Arizona and Stephanie Strassel from the University of Pennsylvania's Linguistic Data Center. Each TLC member will be a regular contributor to the program and will review all major technical issues and consult on the design of the evaluation plan at no additional cost to the government.

2.10.2 Communication Plan

Coordination with the algorithm development teams will occur throughout the program as an integral activity. This coordination will be accomplished through a collaborative process to specify interface specifications and supported system configurations between the evaluation platform and speech processing systems. Documents describing the current understanding and specifications will be distributed electronically, reviewed and revised collaboratively, and maintained in the evaluation program repository available to all RATS program teams. This repository, described in detail below, will be populated during the initial 6 months of the program to contain the latest released version of the evaluation platform software and training data for use in testing by the algorithm teams. Early validation of compliance with the agreed-upon specifications will be ensured by the requirement on the speech processing systems to use

the code repository to maintain the latest code release for integration testing by the evaluation team. This process will result in a set of interim evaluations providing feedback to the algorithm teams and progress reports to the government.

Communication through electronic and telephonic means is anticipated to provide the appropriate opportunities to discuss progress and challenges between the evaluation and algorithm development teams without the necessity for travel outside of the D.C. Metro area. Collaboration with the Data Collection team selected by the government, on the other hand, is anticipated to require monthly in-person meetings during the initial 6-month collection period. These meetings would be used to review the type and mix of training and evaluation data in the context of the scenarios under development, to ensure coordinated data sets and test planning.

SAIC recognizes that there will be significant interest from the scientific community in the RATS program. To this end, SAIC intends to submit summaries of our evaluation design techniques and key learnings for publication in targeted research journals.

2.10.2.1 Evaluation Repository

An Evaluation Repository will be deployed early in the program for communication among the Evaluation Team as a place to track progress on evaluation tasks, post documentation, and share evaluation framework code among members. Once built and tested by the evaluation team, access will be provided to other program participants, including researchers, data team members, and DARPA.

The repository will take the form of a MediaWiki server to which all program participants will be granted read/write access. It will provide several key functions SAIC has found to lead to improved communication between the evaluation team, researchers and DARPA. A document repository allows participants to retrieve evaluation documentation, such as program plans, testing protocols and evaluation framework software documentation, while also

providing a mechanism for sharing feedback on them. A subversion code repository provides access to the RATS Evaluation Framework and a bug tracking database allows researchers to create bug tickets and track the progress of fixes as issues are discovered and fixed throughout the program. In addition to providing feedback on software and documentation all participants can use the wiki itself to create articles of interest to members of the program. The wiki format's ease of editing and creating new articles fosters community within the program and turns the wiki into a hub around which all program activity can be tracked.

At the request of the government, SAIC will offer this program-wide collaboration site based on a similar wiki approach at little or no additional cost. SAIC is also willing to support program-wide mailing lists. These services have been provided on the Machine Reading Program, forming the basis for cross-program and cross-performer interactions and collaboration.

2.10.3 Classified Data Management

Evaluations using classified data will be conducted at the SAIC facility within the appropriately protected environment, with information security oversight and security procedures. SAIC will provide the cleared personnel and resources to manage and execute the evaluations. Analysis, planning, and presentation of the results to the government will occur within the same SAIC facilities. Algorithm teams that include cleared personnel can be invited to out-briefs on evaluation results at the government's discretion.

2.10.4 Program Management Progress Metrics

Our program management team will use SAIC's in-place project management methodology to ensure that we complete all tasks on time and on budget and that deliverables meet or exceed program requirements. We will monitor each task weekly on an integrated project schedule, allowing early identification of potential problems. We will track project resources by task and update them biweekly. Project

management and the TLC will review all deliverables to ensure quality and compliance with requirements.

SAIC has defined interim measures of progress on the evaluation methodology, data preparation, and evaluation framework tasks as shown in **figure 2.10-2**.

Evaluation Task and Metric	Description
Evaluation Methodology	
Percent completion of the evaluation specification (phase 1)	#actual scenarios/#planned
Number of Development Team systems evaluated, by phase evaluation	#unclassified, #classified evaluations
Percent completion of testing by number of partitioned data sets, by phase evaluation	#data sets results returned/#data sets total
Percent completion of testing by total data set audio time in minutes, by phase evaluation	#minutes in data sets results returned/#minutes in data sets total
Ratio of elapsed processing time to audio data set length, averaged over all tests within phase evaluation	(results returned timestamp – test initiation timestamp)/#minutes in data set
Data Preparation	
Amount of audio data examined and annotated, compared to the amount of audio data available (phase 2 classified data annotation task)	#minutes annotated/#minutes in data set
Number and type of annotations by type, classification per time unit, by phase	[#keywords, #speech events, # speakers, #languages]/minute of audio in collection
% completion of data sets partitions available for testing, by type, size, annotation density, by phase	#partitioned data sets complete/#planned
Evaluation Framework	
Percent completion of planned framework revisions (phase 1 task)	#revisions complete/#planned
Number, type, and length of data sets ready and accessible to be used by a system under test through the framework, by phase	#partitioned data sets available/#created
Number of systems that have been installed and successfully undergone integration testing with the framework, by phase	#teams passed testing with framework/#teams total

Figure 2.10-2. Progress Metrics for Evaluation Tasks

For the evaluation methodology, the percent completion of the evaluation specification will indicate the extent to which the team is on schedule to initiate the data preparation and development team evaluation activities. During execution of the end of phase evaluations, metrics will be maintained that show progress toward completing testing across all development teams, and amount of time required to complete each set of test protocols, in first the unclassified and then the classified environment. These include the number of Technical Area 1 Team systems evaluated, percent completion of testing by number of partitioned data sets, and by total data set audio time in minutes, for both the unclassified and classified environments. Time required to complete testing will be reported as the ratio of elapsed processing time to audio data set length measured from test initiation to processing result report completion. As the processing is expected to approach "real-time", this ratio should be close to one, and the overhead for test initiation and closeout will be low as a result of using our automated evaluation framework.

Progress on the data preparation task will be measured for both the annotation and the partitioning activities. Progress on the classified annotation task will be measured as the amount of audio data examined and annotated in minutes, compared to the amount of audio data available. The number and type of annotations by time unit (minutes of audio data) will be tracked to show progress in developing the sample size needed (the number and density of keywords for KWS, for example), for both the unclassified data received from the Technical Area 2 performer as well as the classified data. Partitioning of the audio data into sets with the correct sample size and distribution will be tracked as a percent completion of data sets partitions available for testing, by type, size, and annotation density.

Metrics for the evaluation framework will include both measures of progress in extending the underlying source code and availability of

data sets and Technical Area 1 Team systems for use in performing an evaluation at any time. Progress on the framework development to support the RATS program will be tracked as percent completion of planned framework revisions. Availability of partitioned data sets will be tracked by the number, type, and length of data sets ready and accessible to be used by a system under test through the framework. Availability of the Technical Area 1 Team systems for evaluation will be reported as the number of systems that have been installed and successfully undergone integration testing with the framework, and are therefore ready for performing an evaluation in either the unclassified or classified environment.

2.10.5 Potential Schedule Risk and Risk Mitigation Strategies

For programs such as RATS, which push technology boundaries and pose potential integration challenges, SAIC uses a proactive risk management process. **Figure 2.10-3** identifies potential program risks and SAIC's mitigating strategies.

We will conduct monthly risk assessments to determine when we need to enlist other resources, which may include team-wide, off-bench, in-house expertise. We will create an advisory group that includes senior scientists to conduct regular reviews of progress, future plans, and existing obstacles. We will promptly advise the Defense Advanced Research Projects Agency (DARPA)/Information Processing Technology Office (IPTO) program manager about any risks that potentially affect on-time performance.

2.10.6 Plans and Capability to Accomplish Technology Transition

SAIC recognizes that there is a strong demand within the operational community for the capabilities to be developed in RATS and that one of the goals of the program is to identify and foster transition opportunities. SAIC's technical approach to RATS evaluation will provide a solid foundation, emphasizing the relevance of

	Risk	Risk Level	Impact	Mitigation
	Inability to integrate research algorithms with data and test framework in time to conduct end of phase evaluations	Medium	Medium	Develop test framework that can be used by developers for continuous testing during development, incentivizing continuous integration Provide evaluation framework to performers for on-going integration testing with evaluation system and a representative set of test data
	Inability to execute research algorithms on classified systems	Low	High	Leverage proven process for shift from unclassified -> classified evaluation established over the course of 40+ previous experiences Test on unclassified, mirrored configuration of classified system prior to moving testing in classified environment
	Serious degradation of research algorithms performance in classified environments	Medium	Medium	Test critical aspects of performance – such as trainability on new speakers, keywords, and languages – prior to transition to classified environments
	Difficulty constructing the evaluation framework	Low	Medium	Leverage existing MR Evaluation Framework Use full team's proven evaluation infrastructure expertise and SAIC's extensive system engineering experience to meet initial and evolving requirements

Figure 2.10-3. Risk Analysis Table

RATS technology through scenario-based evaluations and the calculations of MOEs based on MOPs.

In addition, SAIC's broad and deep reach across the intelligence community gives us many opportunities to expose potential customers to RATS technologies for demonstrations and experimentation. Our recommended approach to transition is based on extensive experience

supporting previous technology transitions – including speech analysis technology – into the IC. We believe that this experience, which cannot be discussed within an unclassified proposal, makes us uniquely qualified to support RATS transition. We can provide references to the appropriate contacts within the government upon request.

2.11 Cost Summary

2.11.1 Introduction

SAIC recognizes that the costs associated with each phase of our proposed approach are significantly higher than those described in DARPA BAA 10-34 Amendment 3/ RATS_FAQs_23Mar10.pdf posted on FED-BIZOPS.gov. Our proposed costs are based on our extensive experience on evaluation tasks of similar size, scope, and complexity and are tailored to accomplish key RATS objectives. We believe our higher costs are justified by the following factors, which we view as essential to achieving thorough, effective evaluation of RATS technologies while providing crucial information that will be needed by possible transition partners:

- ◆ Evaluation framework that is shared with algorithm developers and supports continuous testing during development, maximizing program resources by developing shared resource across multiple teams while minimizing risk of integration problems.
- ◆ Experimental design and analysis that breaks down performance across multiple dimensions, identifying strengths, weaknesses,

challenges, and opportunities for different RATS technologies.

- ◆ Scenario-based data collection and evaluation, emphasizing operationally relevant technology development.
- ◆ Streamlined process for moving from unclassified to classified environments during Phases 2 and 3.
- ◆ Method for annotating classified data that is consistent with unclassified data.
- ◆ Estimation of Measures of Effectiveness (MOEs) from Measures of Performance (MOPs) and limited end-to-end testing, allowing potential transition partners to assess the impacts of RATS technologies within the framework needed to justify their investment.

In the case that DARPA feels one or more of these areas are less important, we are prepared to work with the government to select and separate individual tasks where possible, revising our pro-posed approach and costs.

2.11.2 Total Cost Summary by Phase

Figure 2.11-1 presents the Total Cost Summary by Task in Phase 1 and Option Phases 2 and 3.

SAIC Proposal No:

Proposal Title:

Task Title:

Offeror:

Period of Performance:

F00455.A.2311.010.000

Robust Automatic Transcription of Speech (RATS) Technical Area 3 - Evaluation

2.11 Cost Summary - Task & Phase

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION

15 August 2010 - 14 February 2013

2.11 Cost Summary - Task & Phase

Program Tasks	Base Period Phase 1		Option Period 1 Phase 2		Option Period 2 Phase 1	
	Cost	%	Cost	%	Cost	%
WBS 1.1 Develop Evaluation Specification Document	\$137,759	19%				
WBS 1.2 Develop Evaluation Test Framework	\$136,112	19%				
WBS 1.3 Evaluation Test Design	\$164,721	23%				
WBS 1.4 Conduct Phase 1 Evaluations	\$175,463	24%				
WBS 1.5 Management Task	\$103,132	14%				
WBS 2.1 Refine Evaluation Specification Document			\$55,409	11%		
WBS 2.2 Refine Evaluation Framework			\$54,881	11%		
WBS 2.3 Evaluation Test Design			\$101,093	21%		
WBS 2.4 Conduct Phase 2 Evaluations			\$212,049	44%		
WBS 2.5 Management Task			\$63,819	13%		
WBS 3.1 Refine Evaluation Specification Document					\$50,654	13%
WBS 3.2 Evaluation Test Design					\$69,200	18%
WBS 3.3 Refine Evaluation Test Framework					\$35,983	9%
WBS 3.4 Conduct Phase 3 Evaluations					\$171,141	44%
WBS 3.5 Management Task					\$65,467	17%
Total	\$717,187	100%	\$487,251	100%	\$392,446	100%

Figure 2.11-1. Total Cost Summary by Task

2.11.2 Major Tasks and Subtasks by Month

Figure 2.11-2 presents the major tasks and sub-tasks by month.

Note: Second level WBS task and sub-task elements provided only. Greater level of WBS

cost detail can be provided upon request. See Section 2.8 for the activities included under each task and sub-task.

SAIC Proposal No: F00455.A.2311.010.000
 Proposal Title: Robust Automatic Transcription of Speech (RATS) Technical Area 3 - Evaluation
 Task Title: 2.11 Cost Summary - Task & Month
 Offeror: SCIENCE APPLICATIONS INTERNATIONAL CORPORATION
 Period of Performance: 15 August 2010 - 14 February 2013
 2.11 Cost Summary - Task & Month

		Fiscal Year 2010											FY-10	
Program Tasks		Oct-09	Nov-09	Dec-09	Jan-10	Feb-10	Mar-10	Apr-10	May-10	Jun-10	Jul-10	Aug-10	Sep-10	Total
WBS 1.1	Develop: Evaluation Specification Document											\$37,491	\$35,449	\$72,938
WBS 1.2	Develop: Evaluation Test Framework											\$19,923	\$19,923	\$39,846
WBS 1.3	Evaluation Test Design											\$8,605	\$8,605	\$17,210
WBS 1.4	Conduct: Phase 1 Evaluations													
WBS 1.5	Management Task											\$9,049	\$7,643	\$16,692
WBS 2.1	Refine: Evaluation Specification Document													
WBS 2.2	Refine: Evaluation Framework													
WBS 2.3	Evaluation Test Design													
WBS 2.4	Conduct: Phase 2 Evaluations													
WBS 2.5	Management Task													
WBS 3.1	Refine: Evaluation Specification Document													
WBS 3.2	Evaluation Test Design													
WBS 3.3	Refine: Evaluation Test Framework													
WBS 3.4	Conduct: Phase 3 Evaluations													
WBS 3.5	Management Task													
Total		\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$75,067	\$71,618	\$146,686

		Fiscal Year 2011											FY-11	
Program Tasks		Oct-10	Nov-10	Dec-10	Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Total
WBS 1.1	Develop: Evaluation Specification Document	\$28,546	\$12,092	\$12,092	\$12,092									\$64,821
WBS 1.2	Develop: Evaluation Test Framework	\$19,923	\$17,741	\$11,828	\$11,828	\$23,119	\$1,478	\$1,478	\$1,478	\$1,478	\$1,478	\$1,478	\$1,478	\$84,788
WBS 1.3	Evaluation Test Design	\$15,506	\$15,506	\$15,506	\$8,605	\$20,757	\$20,757	\$16,455	\$8,605	\$8,605	\$8,605	\$8,605		\$147,511
WBS 1.4	Conduct: Phase 1 Evaluations													
WBS 1.5	Management Task	\$5,336	\$5,118	\$5,336	\$5,118	\$6,741	\$5,118	\$5,336	\$5,118	\$5,336	\$5,118	\$6,741	\$5,118	\$65,533
WBS 2.1	Refine: Evaluation Specification Document													
WBS 2.2	Refine: Evaluation Framework													
WBS 2.3	Evaluation Test Design													
WBS 2.4	Conduct: Phase 2 Evaluations													
WBS 2.5	Management Task													
WBS 3.1	Refine: Evaluation Specification Document													
WBS 3.2	Evaluation Test Design													
WBS 3.3	Refine: Evaluation Test Framework													
WBS 3.4	Conduct: Phase 3 Evaluations													
WBS 3.5	Management Task													
Total		\$69,311	\$50,457	\$44,761	\$37,642	\$50,617	\$27,353	\$23,169	\$15,201	\$15,419	\$15,201	\$16,825	\$6,596	\$372,653

		Fiscal Year 2012											FY-12	
Program Tasks		Oct-11	Nov-11	Dec-11	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Total
WBS 1.1	Develop: Evaluation Specification Document													\$1,478
WBS 1.2	Develop: Evaluation Test Framework	\$1,478												\$1,478
WBS 1.3	Evaluation Test Design													
WBS 1.4	Conduct: Phase 1 Evaluations		\$41,129	\$67,167	\$67,167									\$175,463
WBS 1.5	Management Task	\$5,336	\$5,118	\$5,336	\$5,118									\$20,907
WBS 2.1	Refine: Evaluation Specification Document					\$25,934	\$16,990	\$12,485						\$55,409
WBS 2.2	Refine: Evaluation Framework						\$14,465	\$14,465	\$12,213	\$6,106	\$4,580	\$1,527	\$1,527	\$54,881
WBS 2.3	Evaluation Test Design					\$8,885	\$15,786	\$15,786	\$16,928	\$21,432	\$13,390	\$8,885		\$101,093
WBS 2.4	Conduct: Phase 2 Evaluations								\$13,242	\$14,973	\$14,973	\$7,487		\$50,675
WBS 2.5	Management Task					\$6,240	\$4,834	\$4,834	\$4,834	\$4,834	\$4,834	\$6,240	\$4,834	\$41,487
WBS 3.1	Refine: Evaluation Specification Document													
WBS 3.2	Evaluation Test Design													
WBS 3.3	Refine: Evaluation Test Framework													
WBS 3.4	Conduct: Phase 3 Evaluations													
WBS 3.5	Management Task													
Total		\$6,814	\$46,247	\$72,503	\$72,285	\$41,059	\$52,076	\$47,571	\$47,217	\$47,346	\$47,777	\$24,138	\$6,361	\$501,395

Figure 2.11-2. Major Tasks and Sub-Tasks by Month

SAIC Proposal No:
Proposal Title:
Task Title:
Officer:
Period of Performance:

F00455.A.2311.010.000
Robust Automatic Transcription of Speech (RATS) Technical Area 3 - Evaluation
2.11 Cost Summary - Task & Month
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION
15 August 2010 - 14 February 2013

Program Tasks	Fiscal Year 2013												FY-13
	Oct-12	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13	May-13	Jun-13	Jul-13	Aug-13	Sep-13	Total
WBS 1.1 Develop Evaluation Specification Document													
WBS 1.2 Develop Evaluation Test Framework													
WBS 1.3 Evaluation Test Design													
WBS 1.4 Conduct Phase 1 Evaluations													
WBS 1.5 Management Task													
WBS 2.1 Refine Evaluation Specification Document													
WBS 2.2 Refine Evaluation Framework													
WBS 2.3 Evaluation Test Design													
WBS 2.4 Conduct Phase 2 Evaluations		\$40,688	\$60,353	\$60,353									\$161,373
WBS 2.5 Management Task	\$4,834	\$4,834	\$6,332	\$6,332									\$22,332
WBS 3.1 Refine Evaluation Specification Document					\$25,237	\$14,444	\$10,974						\$50,654
WBS 3.2 Evaluation Test Design					\$4,563	\$11,464	\$11,464	\$12,822	\$16,292	\$8,032	\$4,563		\$69,200
WBS 3.3 Refine Evaluation Test Framework						\$8,584	\$8,584	\$6,271	\$6,271	\$3,763	\$1,254	\$1,254	\$35,983
WBS 3.4 Conduct Phase 3 Evaluations												\$7,689	\$7,689
WBS 3.5 Management Task					\$6,371	\$4,965	\$4,965	\$4,965	\$4,965	\$4,965	\$6,371	\$4,965	\$42,532
Total	\$4,834	\$45,502	\$66,685	\$66,685	\$36,170	\$30,457	\$35,987	\$34,059	\$27,529	\$16,760	\$12,107	\$13,908	\$389,763

Program Tasks	Fiscal Year 2014												FY-14
	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14	Apr-14	May-14	Jun-14	Jul-14	Aug-14	Sep-14	Total
WBS 1.1 Develop Evaluation Specification Document													
WBS 1.2 Develop Evaluation Test Framework													
WBS 1.3 Evaluation Test Design													
WBS 1.4 Conduct Phase 1 Evaluations													
WBS 1.5 Management Task													
WBS 2.1 Refine Evaluation Specification Document													
WBS 2.2 Refine Evaluation Framework													
WBS 2.3 Evaluation Test Design													
WBS 2.4 Conduct Phase 2 Evaluations													
WBS 2.5 Management Task													
WBS 3.1 Refine Evaluation Specification Document													
WBS 3.2 Evaluation Test Design													
WBS 3.3 Refine Evaluation Test Framework													
WBS 3.4 Conduct Phase 3 Evaluations	\$7,689	\$35,405	\$60,185	\$60,185									\$163,463
WBS 3.5 Management Task	\$4,965	\$4,965	\$6,503	\$6,503									\$22,936
Total	\$12,654	\$40,460	\$66,637	\$66,637	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$186,388

Figure 2.11-2. Major Tasks and Sub-Tasks by Month (continued)

2.12 Organizational Conflict of Interest

Affirmations and Disclosure

In accordance with the instructions in BAA 10-34, Section III.A.1 and Section IVB 2.12, "Organizational Conflict of Interest Affirmations and Disclosure," SAIC affirms that SAIC and our proposed consultant are not currently providing SETA support.

2.13 Human Use

None. Human use is not a factor in this proposal. Should the need arise in the future, SAIC will comply with the federal regulations for human subject protection, DoD 32 CFR 219, *Protection of Human Subjects* and DoD Directive 3216.02, *Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research*. As required, SAIC will provide documentation of a current Assurance of Compliance with Federal regulations for human subject protection and evidence of or a plan for review by an Institutional Review Board (IRB).

2.14 Animal Use

None. Animal use is not a factor in this proposal.

**2.15 Statement of Unique Capability
Provided by Government or
Government funded Team Member**

The SAIC Team does not propose to include any government team member as part of this effort. However, SAIC is willing to work with any government agency or entity designated by DARPA to participate in the RATS program.

**2.16 Government or Government-Funded
Team Member Eligibility**

Not eligible.

APPENDIX A. GLOSSARY

Term or Acronym	Definition
BAA	Broad Agency Announcement
COTS	Commercial off-the-shelf
DARPA	Defense Advanced Research Projects Agency
DoD	Department of Defense
DSRS	Domain-Specific Reasoning System
EARS	Effective, Affordable, Reusable Speech-to-Text
English Text	Text (including automatically transcribed speech) that was originally in English or that was translated into English
GUI	Graphical User Interface
HVI	High Value Individual
IC	Intelligence Community
IPTO	Information Processing Techniques Office
Knowledge Base	Structured information extracted from text
KWS	Key Word Spotting
LCD	Linguistics Data Consortium
LCTL	Less Commonly Taught Languages
LID	Language Identification
LDC	Linguistic Data Consortium
Metric	A numerical measure of performance
MOE	Measure of Effectiveness
MOP	Measure of Performance
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
PE	Performance Evaluation
Pfa	Probability of a false alarm
PI	Principal Investigator
Pmiss	Probability of a missed detection
SAD	Speech Activity Detection
SID	Speaker Identification
Source Language	Language in which the speech or text originated
Speech	Audio signal (digital waveform)
Team	Prime contractor plus 0 or more subcontractors
Text	Ordinary text (in machine readable form) or automatically transcribed speech
T-FIMS	Technical-Financial Information Management System
Total Error (TE)	$TE = 2 (P_{miss}P_{fa}) / (P_{miss} + P_{fa})$
TRL	Technical Readiness Level
TS/SCI	Top Secret/secret compartmented information
User Interface	Software by which users and algorithms interact

APPENDIX B. SECURITY PLAN

This Security Plan presents our approach to supporting the security organization, personnel security, physical security, information security, and operations security requirements of the RATS Program. Our approach will establish a balance between the risk of losing information resources and the inconvenience and cost of security measures. Our goal is to fulfill the overall security objectives of federal statutes and RATS policies and directives, while tailoring specific procedures to meet the needs of the RATS Program to prevent the impeding of scientific and administrative research.

SAIC is cleared by the Department of Defense (DoD) for access to classified information through Top Secret and we have more than 142 SAIC facilities cleared under the National Industrial Security Program (NISP) located in important regional centers throughout the United States. SAIC facilities have been recipients of 28 James S. Cogswell Awards from DoD in recognition of our "Outstanding Industrial Security Program." The DoD has approved SAIC for access to Sensitive Compartmented Information (SCI), Communications Security (COMSEC), Critical Nuclear Weapons Design Information (CNWDI), Restricted Data (RD), North Atlantic Treaty Organization (NATO), and other special access authorizations.

B.1 Approach to Performing Evaluation on Classified Data For RATS Phase 2 and 3

Facility. For this effort, SAIC has selected the building Quincy Street Station, located at 4001 North Fairfax Drive, Arlington, Va. (CAGE Code: 0PSG0). The Air Force Research Laboratory (AFRL) has accredited this facility at the Top Secret level, with areas ranging from Secret to Top Secret for the establishment of our RATS PMO. This building offers SAIC and RATS the best combination of cost, location, and amenities. SAIC selected this building for the RATS contract because it is secured through physical and administrative security mechanisms

and a 24/7 guard force onsite to protect the contents and people in the facility. The AFRL is the certifying authority for the Sensitive Compartmented Information Facility (SCIF) located at the Quincy Street Station. In order for SAIC to receive authorization to use this facility, a Co-Utilization Agreement (CUA) must be in effect between the sponsor of the RATS Program (i.e. DARPA) and AFRL.

Co-Utilization Agreement. The introduction of the evaluation platform into the classified laboratory facility at the 4001 North Fairfax Drive, Arlington VA location requires the strict adherence to a set number of processes. The Air Force Research Laboratory (AFRL) is the certifying authority of the classified laboratory and a Co-Utilization Agreement (CUA) is required prior to the initiation of the classified evaluation process. SAIC will facilitate the establishment of this agreement between the AFRL and DARPA.

System Security Authorization Agreement. Since the evaluation platform will involve Automated Information Systems (AIS), the appropriate Designated Accreditation Authority (DAA) must accredit these systems prior to introducing them into the classified laboratory. A System Security Authorization Agreement (SSAA) will facilitate the certification and accreditation process of the evaluation platform. Once the Evaluation Team has identified the required systems, they will add them to the SSAA and provide them to the certifying authority (i.e. AFRL). The SSAA will document the required security information to support systems certification and accreditation by describing the AIS and providing details surrounding its operation in a secure environment. The scope of the SSAA is to provide a detailed understanding of the AIS concerning security configuration, internal and external connectivity, security countermeasures, threats and vulnerabilities, security administration, and physical layout of the secure environment.

Evaluation Platform. While it is preferred that the Technical Teams furnish their evaluation

systems in software format (i.e. removable media) only, the teams may also furnish equipment as long as the introduced hardware is certified and accredited according to the instructions detailed by the DAA. Furthermore, SAIC will facilitate prior coordination with AFRL to ensure that the Technical Teams introduce this equipment at the earliest stage possible for inclusion into the CUA and SSAA.

Storage of Classified Material. The removable hard-drives and all removable media (e.g. CD-ROMs) provided by the Technical Teams will be permanently stored in the classified laboratory facility at the 4001 North Fairfax Drive, Arlington VA location. SAIC will arrange for additional classified storage containers prior to the initiation of Phase 2 of the DARPA RATS project as needed.

Removal of Evaluation System. At the conclusion of the evaluation, the classified material may be removed from the classified facility as specified by the DAA and the Information System Security Manager.

B.2 Security Organization and Management

For the RATS Program we have designated a facility security officer (FSO) who will also act as the facility manager. The FSO is responsible for directly supporting the security program, including processing security clearances, submitting comprehensive standard operating procedures (SOPs), and implementing the Information Technology Security Plan to control all classified data, equipment, and security training. The FSO has unlimited and complete support and access throughout the life of the RATS Program to two key SAIC business unit individuals: our principal investigator Rich LaValley and our director of security Mr. Bill Tremble, as shown in **figure B.2-1**.

Personnel Security Practices and Procedures, Including Employee Screening Procedures. The SAIC Team meets the RATS Program requirements for processing employees, subcontractors, and consultants for personnel clearances. The SAIC Team will send all completed personnel secu-

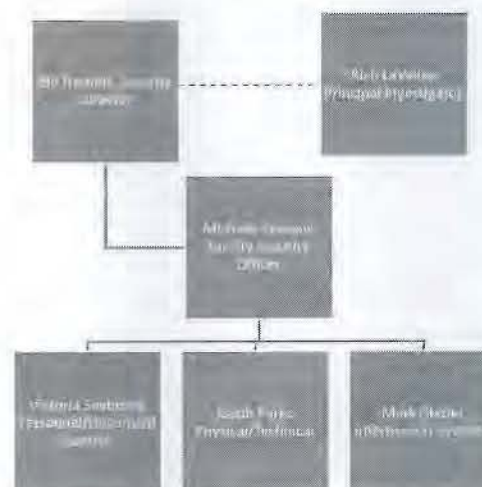


Figure B.2-1 Security Organization Chart

rity-background investigation package to the SAIC security office for tracking and transmission to the DSS. The SAIC Team includes cleared personnel who are currently working on programs that require clearances at the Secret level or higher, and who are available to begin work on Day One of contract award. SAIC policy includes the requirement for each employee with access to attend a series of security awareness briefings to provide them with an understanding of the RATS Program, the role of security on the program, their role relative to security, and our methods and techniques for safeguarding classified information.

B.3 Physical Security Procedures to Protect Classified Data

SAIC will provide physical security for the RATS facility and its subcontractors in accordance with the NISPOM requirements for safeguarding classified material. The safeguards include construction features, access control systems, badging systems, alarms, telephones, and storage facilities. SAIC corporate security, as well as the appropriate government authorities, will inspect each facility on a regular basis to ensure regulatory compliance. Although any of the safeguards alone can only delay attempts to gain unauthorized access to classified information, our combination of safeguards presents a layered, formidable barrier against physical

penetration or inadvertent disclosure of controlled areas. Our physical security safeguard requirements for the Restricted Areas and Closed Areas in which the RATS Program contract activities will take place meet or exceed the physical security construction and administrative requirements established in NISPOM for all Closed Area facilities. To deter and detect unauthorized introduction or removal of classified or sensitive information from the facility, the SAIC Team maintains a formal system that includes random inspection of the personal effects of all persons who enter or exit the facility. The SAIC security office will conduct these inspections at irregular intervals and schedule them so as not to interfere with facility operations. The SAIC security office will prominently display a sign notifying all employees and visitors of this procedure at the primary point of entry.

Procedures for Controlling and Handling Classified/NOFORN Materials. Our extensive experience with other government agencies will serve as the base for all procedures related to controlling, handling, or accessing government data or other classified resources for the RATS Program. The SAIC Team understands that all classified and sensitive RATS work products, including documentation, materials, media, and manuals, become the property of RATS. The SAIC Team will ensure that all materials created, maintained, stored, and transported will do so in a manner that affords protection from unauthorized disclosure. The SAIC Team will handle all data in accordance with established security policies and procedures.

Our security procedures begin with receipt of classified or sensitive data and continue through final turnover of the data. The SAIC Team will track all classified material entering or leaving our facility using our security information management system Access Commander. SAIC currently use this system on other federal contracts and will provide it at no direct cost to the RATS program.

In addition, the SAIC Team ensures that all sensitive material (including data printouts and

other hard copy materials, software documentation, operating manuals, and handbooks) is stored in a secure location when not in use.

All deliverables that contain classified materials that the SAIC Team will send out of the facility will be prepared for transmission using secure communications, hand-carry, or the following procedure: enclose the inner envelope of classification level and ensure sufficient durability and strength to protect the material during transit and mark the outer envelope with the official address provided.

All material released, originated, or reproduced in performing contractual obligations remains the property of the RATS sponsor organization. On completion of each RATS task, the FSO seeks disposition guidance from the contracting officer and the security representative. As required, the FSO prepares a request to retain materials required to fulfill contractual obligations, or, if needed, to perform another RATS task. To prevent unauthorized access or compromise of classified information entrusted to the SAIC facility, the SAIC Team will establish controls for material that is in use and provide approved GSA Class 6 Security Containers or Class 5 Security Containers. SAIC reminds all employees to ensure that non-cleared individuals cannot overhear their classified and sensitive conversations. The SAIC Team will ensure the protection and security of employees operating within open or closed areas via the layout of office furniture and the proper use of screens for computer systems.

Limitations on Employees Concerning Reproduction, Transmission, or Disclosure of Data. The SAIC Team will keep the reproduction of classified deliverable or non-deliverable documents to an absolute minimum, consistent with contractual and operational requirements. The FSO is also responsible for ensuring that only authorized employees carry out reproduction of classified material. Before these employees reproduce any documents, the FSO or security staff will review the documents and determine whether reproducing them is in the best interest of RATS; if not, reproduction of any kind is not authorized.

The FSO also ensures proper recording and accountability of the material after reproduction. We strictly control production and dissemination of these materials. After-hours reproduction is discouraged and must be coordinated with the security staff. If operational requirements dictate such activity, the FSO - in conjunction with the SAIC Team - will establish specific arrangements and procedures on a case-by-case basis.

Procedures for the Destruction of Classified Information. The FSO and security staff member are the only individuals authorized to destroy classified material. The security team will only destroy material with the consent of the program manager and only when the SAIC Team no longer need the material.

B.4 Information Security

Information security addresses the control and monitoring of data used by computer applications and systems. SAIC has developed a DSS-approved System Security Plan (SSP) that defines the procedures for controlling, handling, and accessing government data and other information system resources. This plan follows NISPOM Chapter 8 and other best practice processes. The SSP describes the system and provides details surrounding its operation in a secure environment. The SSP includes detailed descriptions of the system with regard to secu-

rity configuration, internal and external connectivity, security countermeasures, threats and vulnerabilities, security administration, and physical layout. **Figure B.4-1** depicts how the RATS Program and other governing documents correlate with our SAIC management SOP and SSP. This correlation coincides with our approach to tailoring our processes and procedures to accommodate RATS policies and regulations.

The SAIC Team adheres to all information security procedures while processing information in the facility. SAIC enforces security standards that prohibit the use of non-contract-related software on computers used to support this contract. If any non-contract-related software is found on computers supporting this contract, we will investigate the reasons for using the software and bring all computer systems into compliance. Before permitting access to any computing system, SAIC conducts user training and warns system users about restrictions with sign-on warning banners. The SAIC Team gives clear and unequivocal notice to computer users that, by signing on to the system they are expressly consenting to such monitoring. In addition, system administrators monitor computer users in the course of routine system maintenance.



Figure B.4-1. Correlation of SAIC Management SOP and SSP

In addition to the data, the SAIC will secure the operating systems and software used in support of the RATS Program. The SAIC Team applies controls to protect assets from unauthorized or fraudulent use, manipulation, or destruction as required in the areas of auditing, recording, investigating, and archiving. The SAIC Team will also implement security controls for fraudulent or inadvertent occasions; features that guarantee system integrity and prevent unauthorized use of system interfaces; controlled access to the software programs stored in the system; safeguards to protect operational status and subsequent restart integrity during and after a system shutdown. In addition to these security controls, the SAIC will also ensure complete and current documentation that enables us to construct audit trails and implement software features that lock out a terminal not used for a specified period. The SAIC Team will also develop procedural safeguards, such as periodic evaluation of system vulnerabilities, separation of duties, and complete rules for operation; and maintenance processes to validate operating systems before implementation.

In addition to these security measures, SAIC will also implement 256-bit Advanced Encryption Standard (AES) hardware-based encryption on all removable hard drives used during the evaluation process.

As an integral part of our information security process, SAIC automatically backs up data in case of a disaster. SAIC's approach provides integrity and availability through a comprehensive set of requirements and standards for day-to-day protection of data, systems, and software.

Data Backup Procedures. The SAIC Team uses full and incremental backups to meet a variety

of requirements. The SAIC Team will combine full and incremental backups in several ways as solutions to meet specific recovery and business continuity challenges. In a full backup, data is stored on tape or another transportable media in a secure, protected environment. In an incremental backup, all data that has changed since the last full, differential, or incremental backup are stored. The SAIC team will keep incremental backups close to the data center to facilitate restoration in the event of a catastrophic failure.

The SAIC team will back up data every night during non-peak hours. The SAIC Team will maintain incremental backup tapes for four weeks and monthly full backup archive tapes for six months. In addition, as per current operating procedures, SAIC will maintain the last monthly full backup archive for six years or the life of the contract. This scheme provides chronological restoration capability in the event of a disaster or for investigative purposes. Note that SAIC can only restore individual files if they were present on the system during previous a backup operation.

B.5 Operations Security

Operations security (OPSEC) applies to all members of the RATS Program who generate or handle critical program information (CPI) as well as all other sensitive information. We will protect mission-sensitive information, including core mission components such as operational information; maintain classification levels from Unclassified, For Official Use Only (FOUO), and Classified Confidential and Secret; and protect CPI as well as all other sensitive information by analyzing friendly actions attendant to military operations. By developing countermeasures, we not only protect information but also eliminate and minimize indicators.

ATTACHMENT 1. SECURE FACILITY DOCUMENTATION



DEFENSE SECURITY SERVICE
OPERATIONS CENTER - COLUMBUS
P.O. BOX 3488
COLUMBUS, OHIO 43216-3488

May 11, 1999

CAGE: O PSG0

Science Applications International Corporation
Technology Research Group
Attn: Facility Security Officer
4001 N Fairfax Dr., Suite 410
Arlington, VA 22203

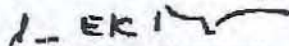
Dear Sir or Madam:

Reference is made to our earlier correspondence regarding the eligibility of your facility for a Department of Defense security clearance. I am pleased to advise that the necessary processing has been completed and a security clearance at the TOP SECRET level is hereby granted your facility.

The fact that your organization has qualified for and has been granted a facility clearance may not be used for advertising nor promotional purposes, nor may this letter be reproduced in any form except for the necessary records of your organization.

The Defense Security Service is vitally interested in assisting you in the development of a sound security posture. We will conduct periodic reviews of your security program to aid you in maintaining proper security safeguards and are available at any time for guidance or assistance.

Sincerely,


JOHN W. FAULKNER
Director

copy: ODCKS

DSS FL 381-R

APPENDAGE TO DEPARTMENT OF DEFENSE SECURITY AGREEMENT


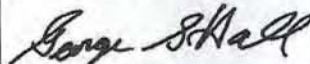
Form Approved
OMB No. 0704-0194
Expires Sep 30, 2007

The public reporting burden for this collection of information is estimated to average 10 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (07040194), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION. RETURN COMPLETED FORM TO YOUR RESPECTIVE COGNIZANT SECURITY OFFICE.

It is further agreed, on this 10th day of December 2007, by and between the United States of America through the Defense Security Service, acting for the Department of Defense, hereinafter called the Government, and Science Applications International Corporation which has entered into the Security Agreement to which this appendix is made a part that the branches and/or facilities listed below, owned and/or operated by said contractor are included in and covered by the provisions of the said Security Agreement, and Certificate Pertaining to Foreign Interests, Standard Form 328

NAME OF PLANT OR FACILITY	NUMBER AND STREET ADDRESS	CITY AND STATE
Science Applications International Corporation (CAGE: 0P5G0)	4001 North Fairfax Drive, Suite 475	Arlington, VA 22203

THE UNITED STATES OF AMERICA BY (Signature of Government Representative)  Nancy de la Garza Field Office Chief	CONTRACTOR (Typed Name) Science Applications International Corporation BY (Signature of Authorized Contractor Representative) 
AUTHORIZED REPRESENTATIVE OF THE GOVERNMENT (Type Name of Government Agency) Defense Security Service (S41SD) 11770 Bernardo Plaza Court, Suite 450 San Diego, CA 92128-2420	TITLE (of Authorized Contractor Representative) George S. Hall, Corporate Security Corporate Industrial Security Manager ADDRESS 10260 Campus Point Drive San Diego, CA 92121

DD FORM 441-1, OCT 2004

PREVIOUS EDITION IS OBSOLETE.

DEPARTMENT OF DEFENSE
SECURITY AGREEMENT

FORM APPROVED
DD FORM NO. 128-0100
EXP. DATE, MAR 31, 1987

THIS DEPARTMENT OF DEFENSE SECURITY AGREEMENT (hereinafter called the Agreement), entered into this 5th

day of January 19 87, by and between the UNITED STATES OF AMERICA, through the Defense Investigative

Service acting for the Department of Defense and other governmental User Agencies (hereinafter called the Government), and

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION

(1) a corporation organized and existing under the laws of the state of Delaware

(NAME OF CONTRACTOR)

(Address of Contractor)

with its principal office and place of business at 10260 Campus Point Drive

in the city of

San Diego

, state of California

(hereinafter called the Contractor)

WITNESSETH THAT:

WHEREAS the Government has in the past purchased or may in the future purchase from the Contractor supplies or services, which are required and necessary to the national security of the United States; or may invite bids or request quotations on proposed contracts for the purchase of supplies or services, which are required and necessary to the national security of the United States; and

WHEREAS it is essential that certain security measures be taken by the Contractor prior to and after being accorded access to classified information; and

WHEREAS the parties desire to define and set forth the promises and specific safeguards to be taken by the Contractor and the Government in order to preserve and maintain the security of the United States through the prevention of improper disclosure of classified information, sabotage, or any other acts detrimental to the security of the United States;

NOW, THEREFORE, in consideration of the foregoing and of the mutual promises herein contained, the parties hereto agree as follows.

Section I - SECURITY CONTROLS

(A) The Contractor agrees to provide and maintain a system of security controls within the organization in accordance with the requirements of the Department of Defense - Industrial Security Manual for Safeguarding Classified Information (hereinafter called the Manual) attached hereto and made a part of this Agreement, subject, however, (1) to any revisions of the Manual required by the demands of national security as determined by the Government, notice of which shall be furnished to the Contractor, and (2) to mutual agreements entered into by the parties in order to adapt the Manual to the Contractor's business and necessary procedures thereunder. In order to place in effect such security controls, the Contractor further agrees to prepare Standard Practice Procedures for internal use, such procedures to be consistent with the Manual. In the event of any inconsistency between the Manual, as revised, and the Contractor's Standard Practice Procedures, the Manual shall control.

(B) The Government agrees that it shall indicate, when necessary, by security classification (TOP SECRET, SECRET, or CONFIDENTIAL) the degree of importance to the national security of information pertaining to supplies, services, and

other matters to be furnished by the Contractor to the Government, or by the Government to the Contractor, and the Government shall give written notice of such security classification to the Contractor and of any subsequent changes thereof; provided, however, that matters requiring security classification will be assigned the least restrictive security classification consistent with proper safeguarding of the matter concerned, since over-classification causes unnecessary operational delays and deprecates the importance of correctly classified matter. Further, the Government agrees that when Atomic Energy information is involved it will, when necessary, indicate by a marking additional to the classification marking that the information is "RESTRICTED DATA." The "Department of Defense Contract Security Classification Specification" (DD Form 254) is the basic document by which classification, marking, and declassification specifications are documented and conveyed to the Contractor.

(C) The Government agrees, on written application, to grant personnel security clearance to eligible employees of the Contractor who require access to information classified TOP SECRET, SECRET, or CONFIDENTIAL.

(D) The Contractor agrees to determine that any subcontractor, subsidiary, individual, or organization proposed for the furnishing of supplies or services, which will involve access to classified information, has been granted an appropriate Department of Defense facility security clearance, which is still in effect prior to providing access to such classified information.

Section II - INSPECTION

Designated representatives of the Government responsible for inspection pertaining to industrial plant security shall have the right to inspect, at reasonable intervals, the procedures, methods, and facilities utilized by the Contractor in complying with the requirements of the terms and conditions of the Manual. Should the Government, through its authorized representative, determine that the Contractor's security methods, procedures, or facilities do not comply with such requirements, it shall submit a written report to the Contractor advising of the deficiencies.

Section III - MODIFICATION

Modification of this Agreement may be made only by written agreement of the parties hereto. The Manual may be modified in accordance with section I of this Agreement.

DD FORM 441 Previous editions of this form are obsolete.

Section IV - TERMINATION

This Agreement shall remain in effect until terminated through the giving of 30 days' written notice to the other party of the intention to terminate; provided, however, notwithstanding any such termination, the terms and conditions of this Agreement shall continue in effect so long as the Contractor possesses classified information.

Section V - PRIOR SECURITY AGREEMENTS

As of the date hereof, this Agreement replaces and succeeds any and all prior security or secrecy agreements, understandings, and representations, with respect to the subject matter included herein, entered into between the Contractor and the Government; provided, that the term "security or secrecy agreements,"

under "agreements and representations" shall not include agreements, understandings, and representations contained in contracts for the furnishing of supplies or services to the Government, which were previously entered into between the Contractor and the Government.

Section VI - SECURITY COSTS

This Agreement does not obligate Government funds, and the Government shall not be liable for any costs or claims of the Contractor arising out of this Agreement or instructions issued hereunder. It is recognized, however, that the parties may provide in other written contracts for security costs, which may be properly chargeable thereto.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and year written above:

THE UNITED STATES OF AMERICA

[Signature]
JOHN E. FOSTER
Director, Industrial Security
(Authorized Representative of the Government)

WITNESS

(Corporation)
By *[Signature]*
J. R. Beyster

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION

(Firm)
Chairman of the Board, President and
Chief Executive Officer

(Title)
10260 Campus Point Drive
San Diego, CA 92121
(Address)

NOTE: In case of a corporation, witnesses not required, but the certificate must be completed. Type or print names under all signatures.

NOTE: The Contractor, if a corporation, should cause the following certificate to be executed under its corporate seal, provided that the same officer shall not execute both the Agreement and the Certificate.

CERTIFICATE

I, J. D. Heipt, certify that I am the Corporate Secretary of the corporation named as Contractor herein; that J. R. Beyster, who signed this agreement on behalf of the Contractor, was then Chairman of the Board, President and Chief Executive Officer of said corporation; that said agreement was duly signed for and in behalf of said corporation by authority of its governing body, and is within the scope of its corporate powers.



[Signature]
J. D. Heipt (Signature)

ATTACHMENT 2. FOCI

CERTIFICATE PERTAINING TO FOREIGN INTERESTS <i>(Type or print all answers)</i>		<i>Form Approved</i> OMB No. 0704-0194 <i>Expires Sep 30, 2007</i>
The public reporting burden for this collection of information is estimated to average 70 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service and Communications Directorate (0704-0194). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.		
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION, RETURN COMPLETED FORM TO YOUR RESPECTIVE COGNIZANT SECURITY OFFICE.		
PENALTY NOTICE		
Failure to answer all questions or any misrepresentation (by omission or concealment, or by misleading, false or partial answers) may serve as a basis for denial of clearance for access to classified information. In addition, Title 18, United States Code 1001, makes it a criminal offense, punishable by a maximum of five (5) years imprisonment, \$15,000 fine or both, knowingly to make a false statement or repre-	sentation to any Department or Agency of the United States, as to any matter within the jurisdiction of any Department or Agency of the United States. This includes any statement made herein which is knowingly incorrect, incomplete or misleading in any important particular.	
PROVISIONS		
1. This report is authorized by the Secretary of Defense, as Executive Agent for the National Industrial Security Program, pursuant to Executive Order 12829. While you are not required to respond, your eligibility for a facility security clearance cannot be determined if you do not complete this form. The retention of a facility security clearance is contingent upon your compliance with the requirements of DoD 5220.22-M for submission of a revised form as appropriate.	2. When this report is submitted in confidence and is so marked, applicable exemptions to the Freedom of Information Act will be invoked to withhold it from public disclosure. 3. Complete all questions on this form. Mark "Yes" or "No" for each question. If your answer is "Yes" furnish in full the complete information under "Remarks."	
QUESTIONS AND ANSWERS		
1. (Answer 1a. or 1b.) a. (For entities which issue stock): Do any foreign person(s), directly or indirectly, own or have beneficial ownership of 5 percent or more of the outstanding shares of any class of your organization's equity securities? b. (For entities which do not issue stock): Has any foreign person directly or indirectly subscribed 5 percent or more of your organization's total capital commitment?	YES	NO
2. Does your organization directly, or indirectly through your subsidiaries and/or affiliates, own 10 percent or more of any foreign interest?	X	X
3. Do any non-U.S. citizens serve as members of your organization's board of directors (or similar governing body), officers, executive personnel, general partners, regents, trustees or senior management officials?	X	X
4. Does any foreign person(s) have the power, direct or indirect, to control the election, appointment, or tenure of members of your organization's board of directors (or similar governing body) or other management positions of your organization, or have the power to control or cause the direction of other decisions or activities of your organization?	X	X
5. Does your organization have any contracts, agreements, understandings, or arrangements with a foreign person(s)?	X	X
6. Does your organization, whether as borrower, surety, guarantor or otherwise have any indebtedness, liabilities or obligations to a foreign person(s)?	X	X
7. During your last fiscal year, did your organization derive: a. 5 percent or more of its total revenues or net income from any single foreign person? b. In the aggregate 30 percent or more of its revenues or net income from foreign persons?	X	X
8. Is 10 percent or more of any class of your organization's voting securities held in "nominee" shares, in "street names" or in some other method which does not identify the beneficial owner?	X	X
9. Do any of the members of your organization's board of directors (or similar governing body), officers, executive personnel, general partners, regents, trustees or senior management officials hold any positions with, or serve as consultants for, any foreign person(s)?	X	X
10. Is there any other factor(s) that indicates or demonstrates a capability on the part of foreign persons to control or influence the operations or management of your organization?	X	X

STANDARD FORM 328 (Revised 7/2004)

PREVIOUS EDITION IS OBSOLETE.