U.S. DEPARTMENT OF
ENERGY

PNNL-18964

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Security Assessment Simulation Toolkit (SAST)

FINAL REPORT

WD Meitzler
SJ Ouderkirk
CO Hughes

November 2009

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

This document was printed on recycled paper.

(9/2003)

PNNL-18964

Security Assessment Simulation Toolkit (SAST)

FINAL REPORT

WD Meitzler
SJ Ouderkirk
CO Hughes

November 2009

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Summary

The Department of Defense Technical Support Working Group (DoD TSWG) investment in the Pacific Northwest National Laboratory (PNNL) Security Assessment Simulation Toolkit (SAST) research planted a technology seed that germinated into a suite of follow-on Research and Development (R&D) projects culminating in software that is used by multiple DoD organizations. The DoD TSWG technology transfer goal for SAST is already in progress. The Defense Information Systems Agency (DISA), the Defense-wide Information Assurance Program (DIAP), the Marine Corps, Office of Naval Research (ONR) National Center for Advanced Secure Systems Research (NCASSR), and the Office of the Assistant Secretary of Defense for Networks and Information Integration (NII), are currently investing to take SAST to the next level. PNNL currently distributes the software to over 6 government organizations and 30 DoD users. For the past five DoD-wide Bulwark Defender exercises, the adoption of this new technology created an expanding role for SAST. In 2009, SAST was also used in the OSD NII International Exercise and is currently scheduled for use in 2010.

While the original concept started as the System Administrator Simulation Training, the value of the technology was quickly recognized, blossoming both in terms of new ideas, applications, and interested sponsors. From the original simulation concept through TSWG investments, the Automated Training Measurement System (ATMS) to quantifiably measure performance emerged, a unique idea in its own right. The initial SAST application idea to train system administrators rapidly expanded to security personnel training, a network range exercise tool, a test and evaluation tool, Information Assurance applications, and Information Operations applications. Over time, contributing sponsors included the Office of Naval Research (ONR), the National Center for Secure Systems Research (NCASSR), the Defense-wide Information Assurance Program (DIAP), the Defense Information Systems Agency (DISA), SAIC, Manakoa, PNNL, and the Department of Energy (DOE).

As a result of technology transfer achievements, PNNL has four active SAST projects with a research value in excess of $1.6M today. PNNL anticipates the research sponsor value to expand by $1.5M this year. Thus the total SAST R&D for fiscal 2010 is estimated at $3.0M. The DoD TSWG investment including DIAP co-funding was $1.1M in fiscal year 2009.

Acknowledgments

PNNL wishes to thank DoD TSWG for sponsoring the very successful SAST research. This year’s primary project objective for technology transfer was clearly achieved with follow-on research sponsorship in excess of $1.5M and the application of the capability expanding within the DoD community. To the many organizations and staff who contributed, sponsored, and/or used the SAST technology, we extend our appreciation.

Acronyms and Abbreviations

ANTS	Automated Network Traffic Synthesizer
ATMS	Automated Testing Measurement System
CAT	Coordinated Attack Tool
CEMAT	Consolidated Exercise Metrics Analysis Tool
CIPS	Critical Infrastructure Protection Simulator
CSF	PNNL's Computer Science Facility
DIAP	Defense-wide Information Assurance Program
DISA	Defense Information Systems Agency
DoD	Department of Defense
IA	Information Assurance
IO	Information Operations
IP	internet protocol
JITC	Joint Interoperability Test Command
LDRD	Locally Directed Research and Development
MUTT	Multi User Traffic Tool
NCASSR	National Center for Advanced Secure Systems Research
ONR	Office of Naval Research
OSD NII	Office of Secretary of Defense International Exercise Program
PNNL	Pacific Northwest National Laboratory
R&D	Research and Development
SAST COI	Community of Interest
SAST	Security Assessment Simulation Toolkit
SEAL	SAST Secure Environment for Accelerated Learning
TSWG	DoD's Technical Support Working Group

Contents

Summary iii

Acknowledgments v

Acronyms and Abbreviations vii

1.0 Introduction 1

2.0 Background 1

3.0 Why 1

4.0 Concept Overview 2

5.0 Outcome 4

Appendix A – SAST Flier A.1

Appendix B – SAST Presentations B.1

Appendix C – SAST Software Release C.1

Appendix D – Financial Information D.1

Figures

1 Concept Overview 2

2 SAST Software Distribution 5

3 SAST Research Sponsors 6

1.0 Introduction

The Security Assessment Simulation Toolkit (SAST) Final Report provides an overview of the R&D performed by Pacific Northwest National Laboratory (PNNL) and the outcomes resulting from the Research and Development (R&D) investment. The report appendices contain SAST-related communication materials including a one-page brief, a presentation, and financial information. The included SAST 3.2.1 software distribution contains expanded documentation and the software.

2.0 Background

The initial SAST concept was derived from the PNNL Critical Infrastructure Protection Simulator (CIPS) Locally Directed Research and Development (LDRD) conceived by Wayne Meitzler whose goal was to simulate all aspects of the national infrastructure. The SAST concept reduced the CIPS scope to the information infrastructure. At the time, computer security concerns were rising and system administrators had almost no security training or experience. To fulfill this gap, the SAST research project was born. The training community started building security training content, courses, and computer aid instruction. This provided security information to the student, but a critical void in security experience remained. Rapidly developing this crucial security experience in a compressed timeframe became the primary goal for the SAST research.

As the SAST research concepts were shared in the community, the research team recognized that the fundamental SAST capabilities had applications beyond training system administrators. Over time, five viable applications (Figure 1) for SAST were identified, creating a generic suite of tools with many security applications. Concurrently, the user community has started using the SAST components to address a variety of problem sets. PNNL has established a SAST Users Group to help collect requirements, share solutions, and provide training.

After two years of development for the Department of Defense's (DoD's) Technical Support Working Group (TSWG) SAST project, the software has been distributed to government, academia, and internationally requestors with positive feedback and increased interest for additional features.

3.0 Why

Most government agencies and the DoD community have a compelling need to protect their information infrastructure on which their critical software depends for all aspects of their operations, be it a weapons system, logistics, or command and control. This need is based on the fact that few can really return to their manual means for doing business.

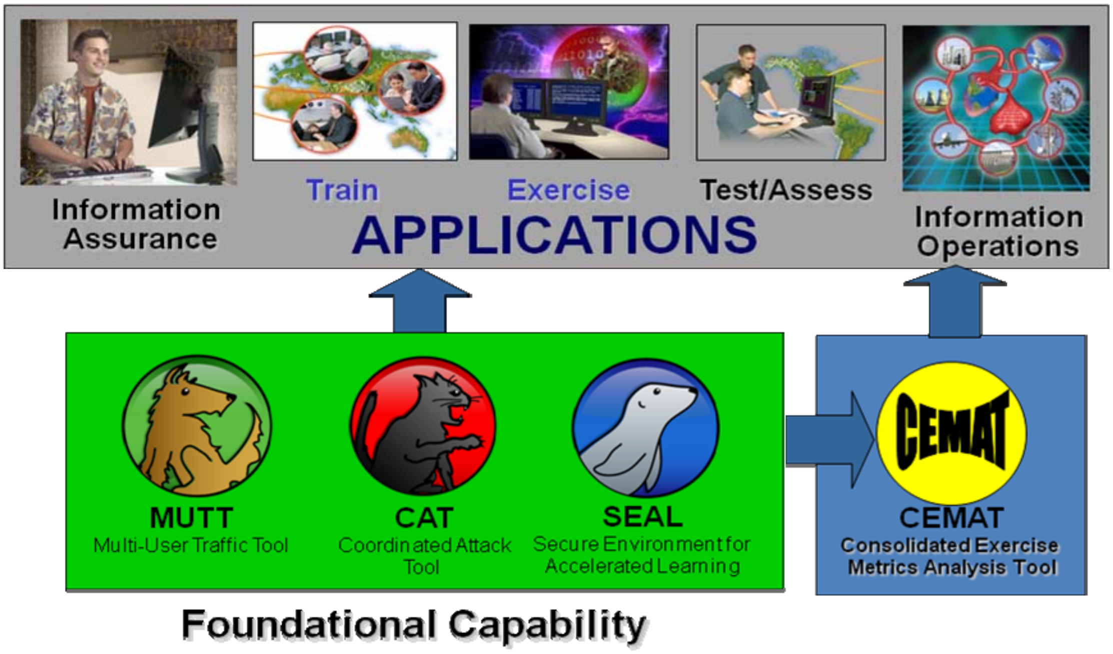


Figure 1. Concept Overview

In the cyber security world, usually the best defense is the most experienced professional. An automated tool to fully protect simply does not exist. With staff placed in these positions almost right out of school, and rotating quickly, there is usually an experience deficiency, thus the compelling need to rapidly build experience, a primary objective for SAST.

In addition, organizations use various products for each element of security including training, testing, information assurance, and information operations. This results in the acquisition of multiple products that are often not interchangeable and each may require specific training. The net effect is that training becomes required for each tool, and repeated each time a staff member rotates usually in a two-year cycle. All of this drives the need for a more generic interchangeable capability for all security applications (training, testing, Information Assurance [IA], Information Operations [IO]) that is easy to use reducing labor costs and complexity.

4.0 Concept Overview

The SAST concept is one cyber simulation tool for many aspects of cyber security. Essentially, it is the exact same tool used for training, exercises, testing, evaluation, IA, and IO. Figure 1 shows these applications and their relationship to the core SAST components.

The SAST foundation is based on a modular software design to provide this extensive capability for all applications. The SAST components may be used collectively or individually based on ones requirements.

Computer simulations are most commonly used to gain a better understanding of the underlying processes for a wide variety of problem domains. A cyber security simulator is comprised of three elements; the network infrastructure, the network traffic flows, and network instrumentation.

The infrastructure element consists of all fixed components in the network range, including hardware (workstations, switches, and routers), software (operating systems, and applications), and topology (inter-device connectivity, routing tables). The network infrastructure, also called the network range (or range for short), can be represented by physical, emulated, virtual, and simulated components. Which of these is chosen will depend on the nature of the experiment. In general, actual physical components provide the greatest fidelity and least scalability, while simulated components provide least fidelity and greatest scalability, with emulation and virtualization providing intermediary properties. This is the environment in which SAST is intended to operate and, while SAST provides some guidance on how such environments might be created, it is intended that SAST be operational on a wide variety of network range designs to provide the greatest flexibility.

The network traffic flows represent the dynamic behavior of the network range resulting from the expected operation of the network by users and devices on the range. User-generated flows can be the result of a variety of behaviors, both authorized and unauthorized. Authorized behaviors may include, but are not limited to, sending and receiving email, web surfing, file transfers, and remote authentication. Unauthorized behaviors may include policy violations (going to unapproved site, sending unauthorized emails), and malicious activities (scanning, privilege escalation, data exfiltration, worms, viruses, trojans). Device-generated flows can also result from a variety of actions such as automated backups, time synchronization, logging, system patches, and updates. SAST provides network traffic flow functionality through the Automated Network Traffic Synthesizer (ANTS) with plug-in modules to achieve the Multi-User Traffic Tool (MUTT) and Coordinated Attack Tool (CAT) capability. Many consider the MUTT traffic acceptable activities and the CAT traffic malicious, bad, or failed activities

ANTS functions by creating synthetic representations of people and devices called actors. These actors carry three attributes: a specification data set, an activities (work) schedule, and a task plan. The specification data set provides information that defines the properties of the actor such as internet protocol (IP) address, MAC address, email account, authentication credentials, and any other information necessary to perform the assigned tasks. The activities schedule defines the time-based operations state of the actor such as working, at lunch, or on break. These activities can be probabilistic for likelihood of occurrence and (if it occurs), the start and end of the activity. The task plan specifies the actions and action rate to be performed before, during, and after an activity. Tasks may include surfing the web, sending or receiving email, uploading or downloading files, authenticating to a server, or any other behavior provided by ANTS. Just as with the schedule, tasks action rates and targets can be deterministic or probabilistic. ANTS currently provides sixteen different engines to perform network actions and is designed to support engine plug-ins to provide new capabilities as needed. ANTS is capable of creating hundreds of actors on a single host, thereby allowing the simulation of large networks with relatively little hardware.

Range instrumentation includes two components, a range management system and a range monitoring system. The range management system provides the operator(s) with the ability to access, view, and control range assets, as well as provides a means to incorporate live actors into the simulation when needed. The range monitoring system provides the means for the operator(s) to continuously measure the state of the simulation and collect metrics for analysis.

The SAST Secure Environment for Accelerated Learning (SEAL) component provides the range management functionality. It allows the operator to provide multiple views and control of range assets from both local and remote access points. The range access can be compartmentalized to provide for conducting multiple distinct experiments (e.g., training sessions) or interactive sessions (e.g., war games). Access to the range through SEAL can be shared among over 100 people, and control of any range resource may be dynamically reassigned to any authorized user.

The Automated Testing Measurement System (ATMS) component provides the range monitoring system. ATMS provides the tools necessary to inject, detect, and record network tracer packets for a variety of data types to provide real time analysis of network traffic flows through predefined control points. These control points represent points of interest within the network where changes in the nature of traffic flow can be used to infer the underlying nature of the network. In a typical application of ATMS, at least two kinds of traffic flows will be tagged: authorized traffic, which should always flow, and unauthorized traffic, which should be blocked at control points. By analyzing these two flows, the condition of the network and the effectiveness of the security can be determined.

The Concept Overview in Figure 1 provides the Consolidated Exercise Metrics Analysis Tool (CEMAT) for completeness. CEMAT is a Joint Interoperability Test Command (JITC) capability to track and measure security performance. Plans are in place for SAST components to interface and exchange data with CEMAT at the conclusion of 2010.

5.0 Outcome

The outcome of the SAST DOD TSWG-sponsored research can be measured in terms of an established sponsor base, an establish capability user community, a software product, and a supporting product infrastructure. Each of these elements contributes to the last project funding increment emphasizing technology transfer. More information on each of them follows.

The current software product is SAST 3.2.1 and is distributed either through a direct download or CD distribution, depicted in Figure 2. While the DoD TSWG SAST project is now complete, subsequent sponsored research is in progress that will result in subsequent software releases. As a minimum, a new release of the SAST SEAL component is expected in the next quarter.

FOR OFFICIAL USE ONLY
System Administrator Simulation Trainer (SAST)
Secure Environment for Accelerated Learning (SEAL)
SAST Example Network Services Version 1.0
Coordinated Attack Tool (CAT) Version 1.3
Multi-User Traffic Tool (MUTT) Version 2.2
IPAL
Battelle

Figure 2. SAST Software Distribution

The supporting SAST software infrastructure is evident by the SAST R&D team at PNNL which is engaged in 5 SAST projects and a SAST laboratory established in the new PNNL Computer Science Facility (CSF) that just opened in October 2009. Sponsorship of on-call technical support is also in place.

The established SAST user community outcome is evident by the use of SAST in the last five Bulwark Defender Exercises, the last NII International Community exercise, the broad range of use in the Marine Corps, and the distribution of the software to six government organizations involving approximately thirty users. Within the next 6 months, the SAST software along with a suite of user community features will be available through the SAST Community of Interest (SAST COI) website currently planned through project.mil, a website hosted by Defense Information Systems Agency (DISA).

The sponsor base outcome is clear as a result of the DISA IA Range SAST R&D sponsorship. Through the DISA program manager, Rob Powell, a smooth technology transfer is in progress with a $1M project in progress and a $1.5M investment planned for early FY 2010. The collective sponsors for SAST at this time are DISA, the Defense-wide Information Assurance Program (DIAP), the Marine Corps, Office of Naval Research (ONR) National Center for Advanced Secure Systems Research (NCASSR), and the Office of Secretary of Defense International Exercise Program (OSD NII). Collective R&D funding in place is $1.6M today, with another $1.5M expected yet this calendar year. So the follow-on funding to this project will exceed $3M by the end of the calendar year.

Participation in government events over the course of the year included:

- USMC IA Conference participation, March 2009
- International IA exercise/participation, June 2009
- Bulwark Defender, October 2009
- Mohave Viper Participation, August 2009
- AFIT SAST internship, September 2009

Figure 3 provides a graphic summary for sponsors over time for the PNNL SAST technology. The chart uses the sponsoring organization abbreviated name and the high level project title.

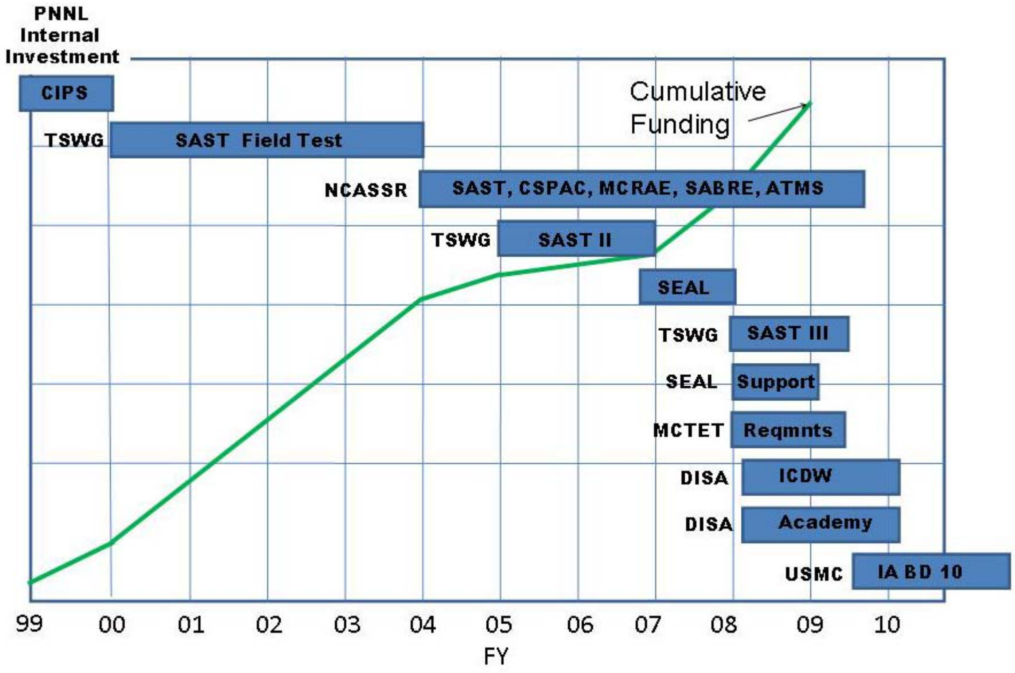


Figure 3. SAST Research Sponsors

The PNNL research team wishes to thank the many organizations and staff who contributed, sponsored, and/or used the SAST technology. This DoD TSWG investment provided the seed for substantial advancement and application of this technology in the future.

Four appendices to this report provide additional information on the SAST projects:

- Appendix A – SAST Flier
- Appendix B – SAST Presentations
- Appendix C – SAST Software Release
- Appendix D – Financial Information

Appendix A

SAST Flier

SAST

(Security Assessment Simulation Toolkit)

Anyone who depends on computers, networks, or digital devices faces increased risk through vulnerabilities that can substantially impact if not disrupt their mission. These can include hardware, software and network attacks by adversaries or catastrophic failures.

VULNERABILITY RISK FACTORS INCLUDE:

- *increased sophistication of stealthy attacks*
- *rapidly changing threats*
- *insufficient numbers of highly qualified, security personnel*
- *lack of adequate capabilities to measure security performance*
- *substantial pressures to reduce security costs while improving performance*
- *uncertainty of vulnerabilities.*

OPPORTUNITY

The Security Assessment Simulation Toolkit (SAST) offers a suite of simulation tools directly applicable to cyber security training, exercises, testing, evaluation, information assurance and information operations. Figure 1 depicts many of the applications possible, along with the core SAST components that make it a reality.

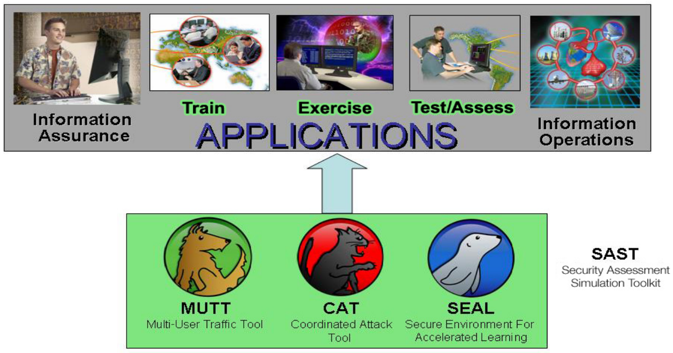


Figure 1. Foundational Capability

As a training tool, security personnel can use SAST directly via a network range to rapidly build experience in cyber security augmenting traditional training programs. SAST allows you to train as you operate, or in the case of DoD, train as you fight. It is valuable to refresh security skills at the user's convenience and rapidly update skills when new exploits emerge.

MUTT and CAT, each components of SAST, provide network traffic flows with far greater realism than exists through any other means for exercising cyber security defenses. Furthermore, they enable the effective use of network ranges for many critical security applications. SAST scales from exercising small units up to large, multiple organizations at the national level.

For testing and evaluation, SAST makes possible the ability to measure the individual or collective performance of cyber security tools or personnel. Such capability affords great value when evaluating the effectiveness of one's own defensive posture; when adopting new methods or evaluating new tools to determine their collective effectiveness.

Pacific Northwest
NATIONAL
LABORATORY

SAST
Closest thing to reality without being there

- One tool suite, many security applications
- User autonomy
- Scalable
- Interoperable among computational environments
- Software/hardware independence
- Rapid experience building

U.S. DEPARTMENT OF ENERGY

SCIENCE -BASED SOLUTIONS FOR NATIONAL SECURITY

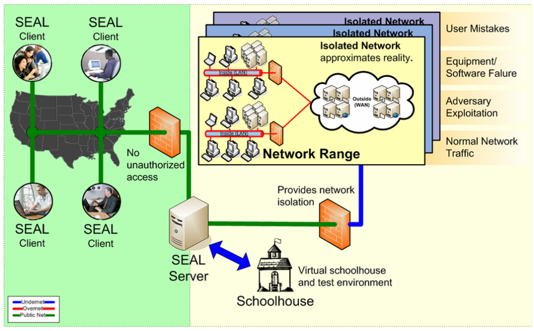


Figure 2. SAST Concept

Fundamental principals of SAST include:

- *full user autonomy for tool use*
- *performance measurement*
- *scalability from a few computers to a massive network*
- *virtual equipment (eg: computers)*
- *virtual people*
- *interoperability across many computational platforms and networks*

The fundamental SAST concept [Figure 2] for all applications involves the use of the SAST core capabilities (MUTT, CAT, SEAL) [Figure 1] in conjunction with a network range [Figure 2]. The network range approximates reality through the use of real computers, networks, switches, firewalls, synthetic people, and exploits. Essentially the SAST software virtualizes the user community by synthesizing peoples' behavior to generate the associated traffic and subsequently allows for a level of interaction not possible with other technologies. SEAL, via its clients, makes access to the SAST range possible anywhere in the world. A brief description of the major SAST components follows:

Multi-user Traffic Tool (MUTT): offers the capability to model the actual behavior of the population of network users and organizations individually or collectively to any level of fidelity desired by the user. It can simulate scenario-based schedules and timeframes. From the model, MUTT automatically generates complete session network traffic from any one or more computers in the network range up through total network saturation.

Coordinated Attack Tool (CAT): offers the capability to directly insert malicious exploits into the network and computational environment as well as user and equipment failures or errors. CAT automates most of this process while allowing operator intervention.

Secure Environment For Accelerated Learning (SEAL): offers the capability to remotely access the SAST simulation environment from any where Internet or network services exist, along with the ability to customize views in the network range depending on the roles a user plays. Furthermore, a user can obtain a multi-dimensional view of a cyber attack via SEAL.

AVAILABILITY

SAST or any of its components are available license-free in the form of a 4-CD set to government agencies. Live demonstrations of SAST are available at Pacific Northwest National Laboratory (PNNL). New features are currently in development and will become available through semi-annual software releases.

SPONSORS

The Department of Defense (DoD), Technical Support Working Group (TSWG); Defense-wide Information Assurance Program (DIAP); Office of Naval Research (ONR); National Center for Advanced Secure Systems Research (NCASSR); Defense Information Systems Agency (DISA); and the Department of Energy (DOE) sponsored the research that makes the SAST capability possible.

Any government organization can directly leverage these substantial investments or choose to move this technology forward should they have unique requirements to defend the integrity of their computer and network systems. The SAST program shares the outcomes of its research and resulting products with all of the SAST partners.

To receive the benefits of becoming a SAST partner and learn more about how your organization can become a part of this team, please contact the individual listed below who will be happy to assist you.

ABOUT PNNL

Pacific Northwest National Laboratory, a U.S. Department of Energy Office of Science laboratory, solves complex problems in energy, the environment, and national security by advancing the understanding of science. PNNL employs more than 4,000 staff, has a business volume of $750 million, and has been managed by Ohio-based Battelle since the Lab's inception in 1965.

For more information contact:

Wayne Meitzler
Cyber Security R&D Program Manager
Pacific Northwest National Laboratory
P.O. Box 999, MSIN K8-41
Richland, Washington 99354
Phone: (509) 375-3718
Secure Phone: (509) 372-6815
Fax: (509) 375-6644
wayne.meitzler@pnl.gov
SIPR: wayne.meitzler@pnnl.doe.sgov.gov
www.pnl.gov

Pacific Northwest
NATIONAL LABORATORY

Appendix B

SAST Presentations

SAST

Security Assessment Simulation Toolkit

Wayne Meitzler
Steve Ouderkirk
Chad Hughes

Pacific Northwest NATIONAL LABORATORY

PNNL-SA-67718

The Essence

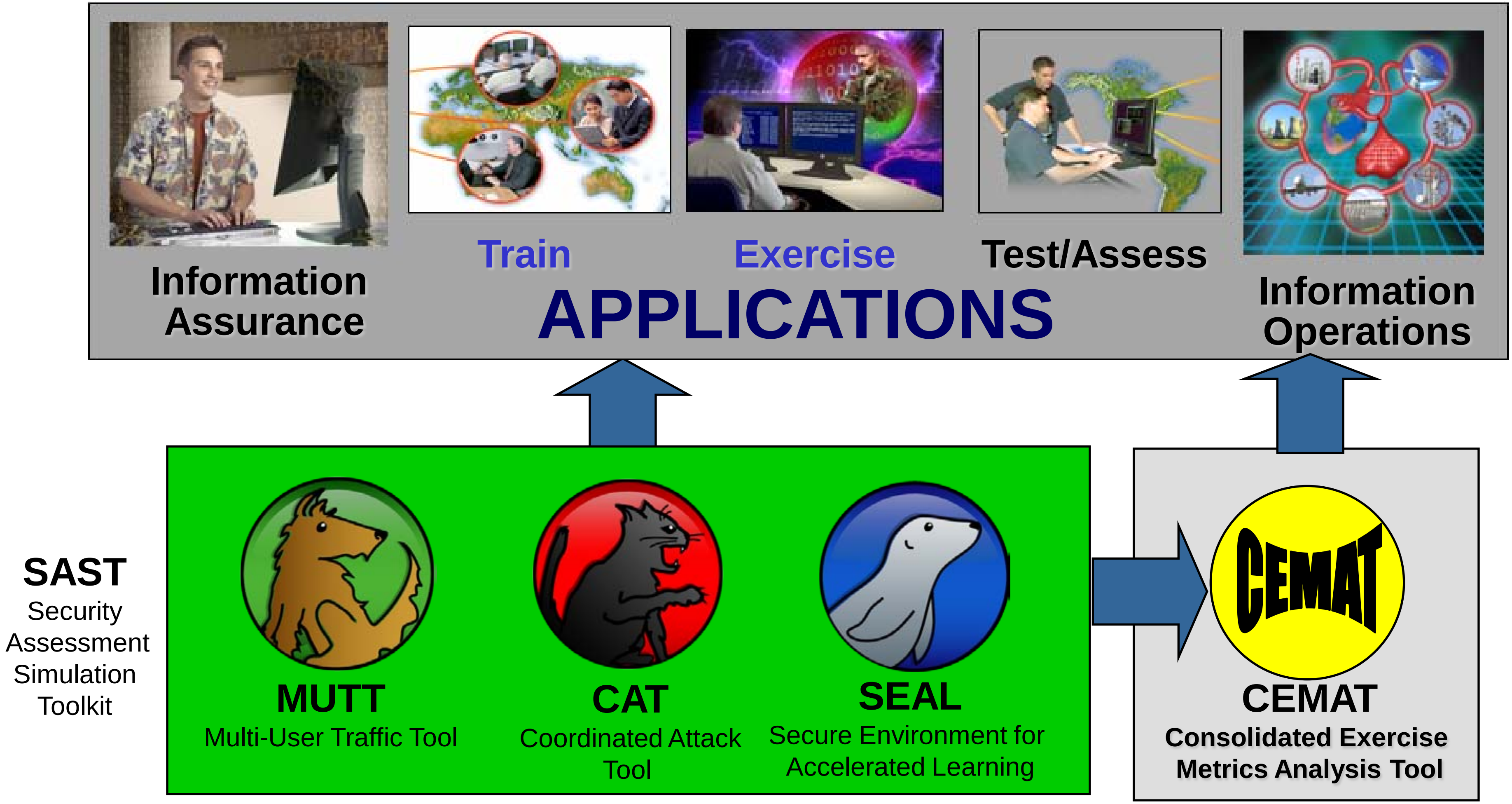
Provide the closest thing to reality for the cyber world without the expense, risk, and complications of being there.

Train, test, & exercise as you fight

Brings a live-fire exercise to the IA and IO community

Pacific Northwest
NATIONAL LABORATORY

Use



Information Assurance

Train

Exercise

Test/Assess

Information Operations

APPLICATIONS

SAST
Security Assessment Simulation Toolkit

MUTT
Multi-User Traffic Tool

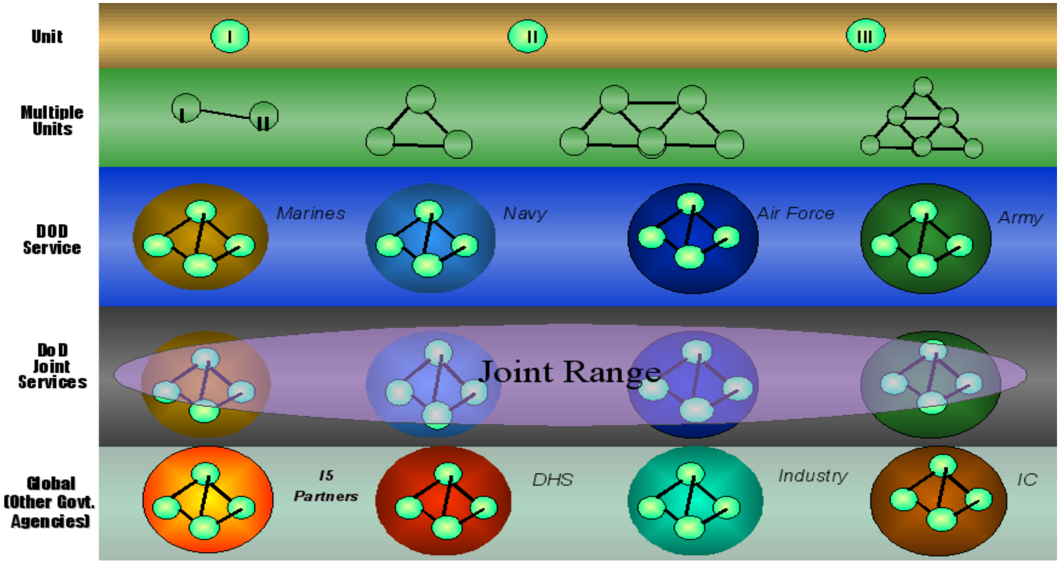
CAT
Coordinated Attack Tool

SEAL
Secure Environment for Accelerated Learning

CEMAT
Consolidated Exercise Metrics Analysis Tool

Foundational Capability

Guiding Principles

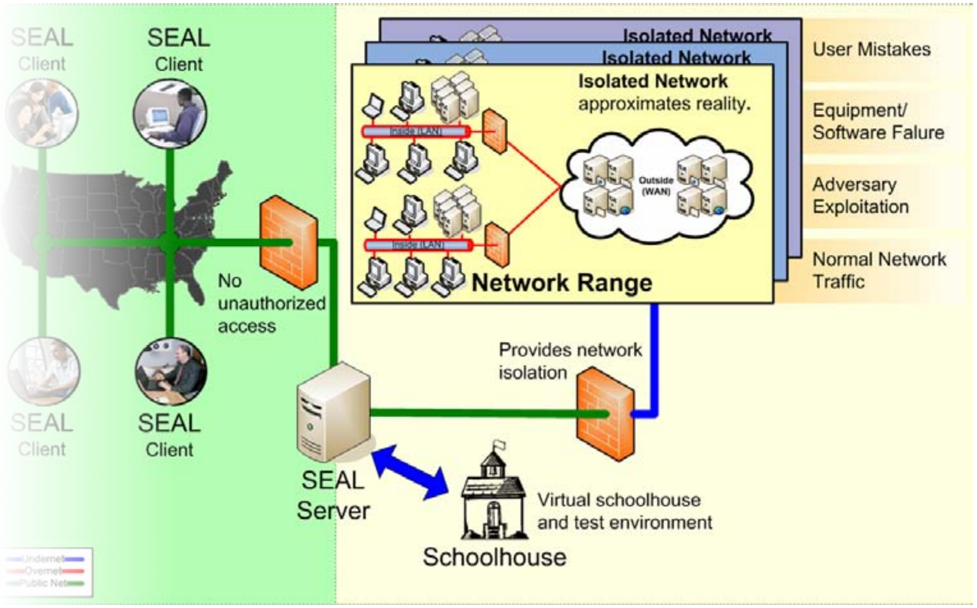


- User Autonomy
- Scalable
- Multi-platform
- Multi-use
- Lower Costs
- No software licenses
- Available to any government agency with the signing of a typical Government User Agreement (GUA)
- Shared investment outcomes

Pacific Northwest
NATIONAL LABORATORY

Concept

- Approximate reality
  - Network environment
  - Virtual people, hardware, & software
  - Based on operational objectives
  - Real traffic
- Partition and individually control range resources
- Isolate range from production systems
- Offer multiple points of presence within the range
- Aggregate multiple geographically dispersed ranges



Pacific Northwest
NATIONAL LABORATORY

Multi-User Traffic Tool (MUTT)

- Synthesizes people that produce realistic normal network traffic
  - Perform realistic activities
    - Email, web surf, FTP, Active Directory, etc.
  - Exhibit realistic behaviors:
    - Work schedules, personalities
    - Content database (e-mail, URLs, files)
    - Schedule (stochastic by time/day)
    - Population size (stochastic by time/day)
- Each host can simulate
  - One to two hundred virtual people
  - Unique behavior profile
  - Unique IP and MAC addresses
- Provides traffic flows at all levels to include saturation

Pacific Northwest
NATIONAL LABORATORY

Coordinated Attack Tool (CAT)

- Synthesizes people to produce realistic malicious traffic
- Perform real-world attacks
  - Cover fire
  - Smoke screen
  - Reconnaissance
  - Naive users
  - System failures
- Perform distributed attacks internally and externally
  - Outsider and insider threat
  - Script kiddies and naive users
- Augment live red teams

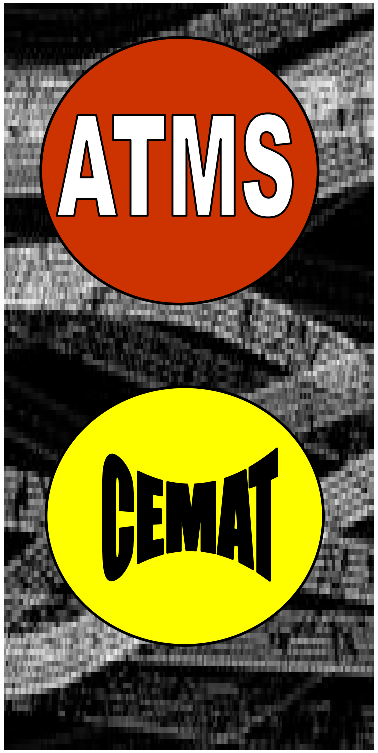
Pacific Northwest
NATIONAL LABORATORY

Secure Environment for Accelerated Learning (SEAL)

- Provides controlled range access
  - Multiple points of presence
  - Many-to-many control of resources and views
  - Dynamic allocation of range resources
  - Participants do not need to be co-located with each other or the classroom.
- Protects and isolates the range
  - All communications are encrypted
  - Participant machines are isolated from the range
  - Malicious codes are constrained to the range
- Offers a virtual university
  - Multiple courses
  - Information repository and collaboration
- DISA pilot in progress

Automated Test Measurement System (ATMS)

- Selected network traffic is tagged with an identifier that indicates the nature of that traffic
  - At a minimum this would be authorized and unauthorized
- Sensors are deployed at multiple points of interest within the network range to measure tagged traffic flows in real time
- Monitors are deployed to aggregate, report, and analyze the flows of tagged traffic with the results delivered to CEMAT

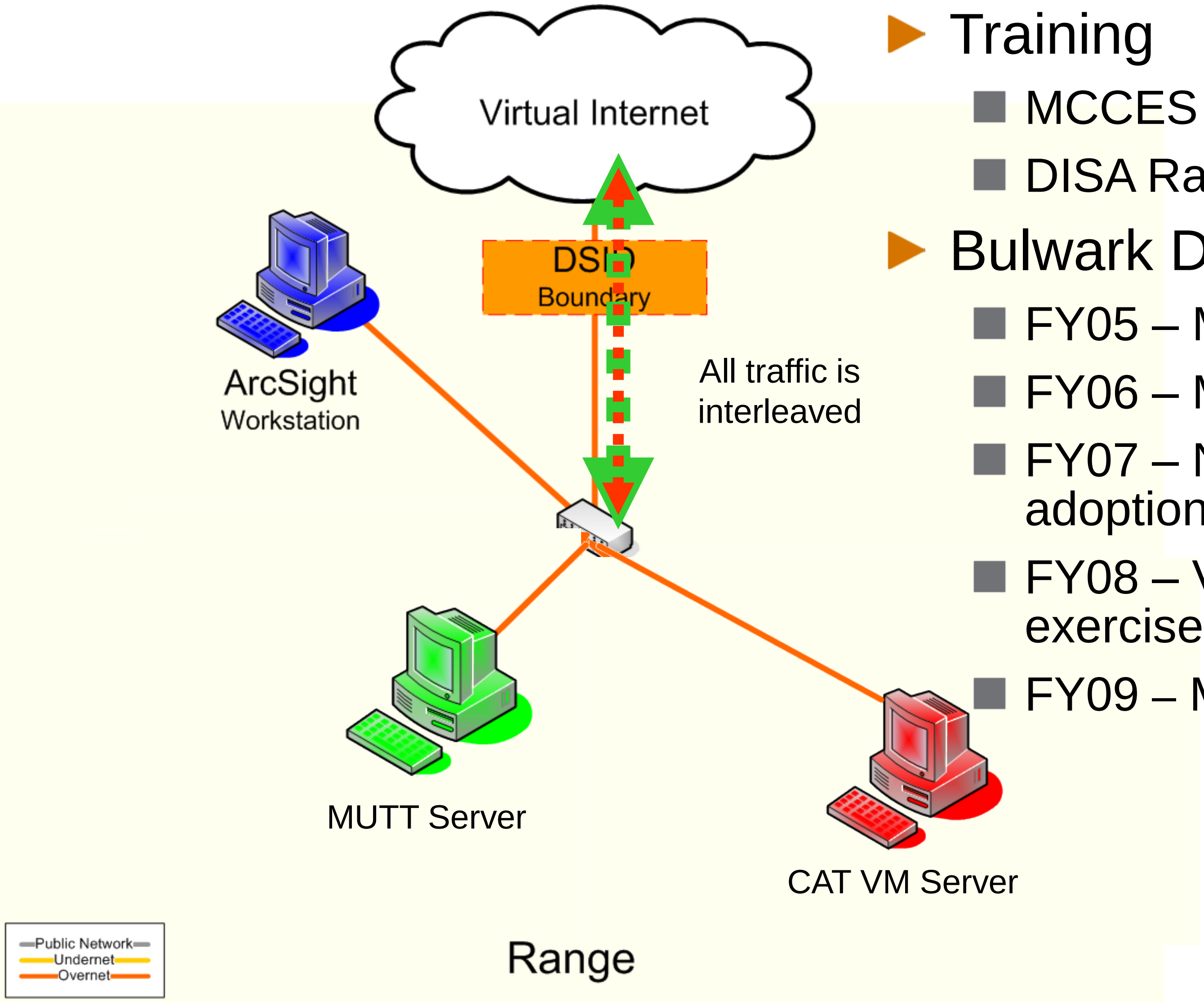


SAST Software

- Independent testing
- Unified CAT and MUTT GUI
- API for creating virtual people and associating activities to them
- New modular scenario design
  - Actors own their credentials
  - Systems own their IP and MAC
- Ability to assign a single virtual person to a specific VM
- Easier scenario management
  - Building scenarios
  - Sharing scenarios

FOR OFFICIAL USE ONLY
System Administrator Simulation Trainer (SAST) 1.9
Secure Environment for Accelerated Learning (SEAL) Version 1.3
SAST Example Network Services Version 1.0
Coordinated Attack Tool (CAT) Version 1.3
Multi-User Traffic Tool (MUTT) Version 2.2
IPAL
Battelle

IA Training and Exercise Examples



- Training
  - MCCES Pilot FY04-FY05
  - DISA RadX Pilot FY09
- Bulwark Defender
  - FY05 – MCCES
  - FY06 – MCNOSC
  - FY07 – Navy NIOC adoption
  - FY08 – Virtual MCEN exercise
  - FY09 – MCNOSC

Questions?

Wayne Meitzler

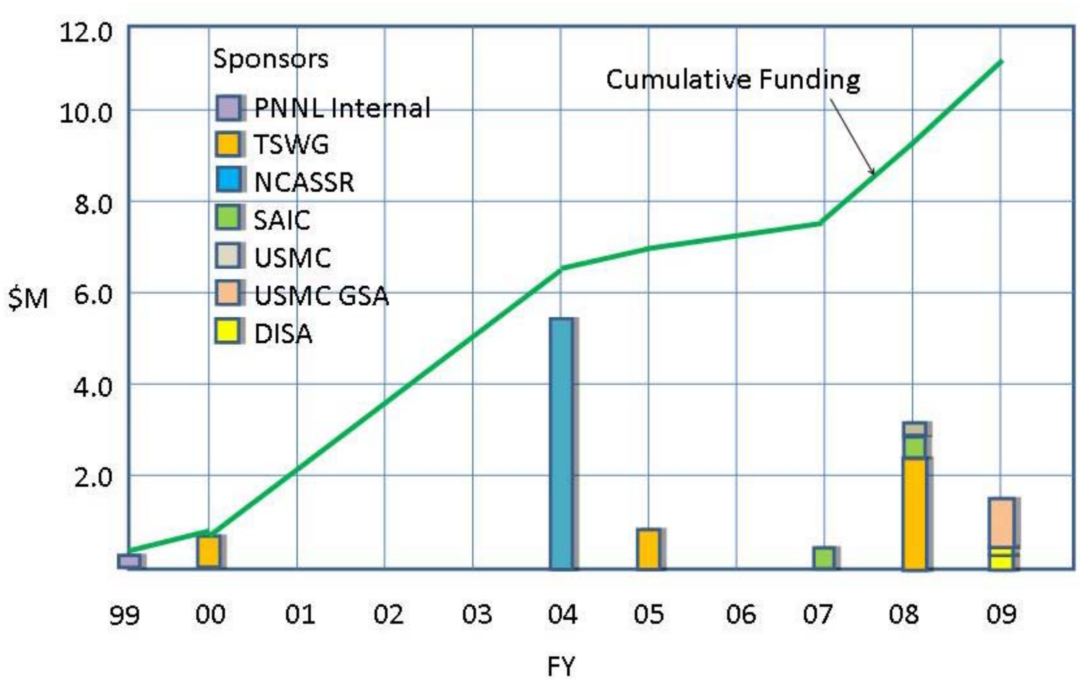
SAST Program Manager
Pacific Northwest National Laboratory (PNNL)
P.O. Box 999, Mail Stop K8-41
Richland, WA 99352
Phone: (509) 375-3718
Mobile: (509) 392-2066
E-mail: wayne.meitzler@pnl.gov
SIPR: wayne.meitzler@pnnl.doe.sgov.gov

Appendix C

SAST Software Release

Appendix D
Financial Information

The following chart and table provide the financial history of the program from 1999 to the present.



Sponsor Overview over Time

Detailed Budget Information Relative to SAST Projects, 2000-2009

		Value ($)	Start	End	
41129	SAST	538,272.01	6/14/2000	9/30/2004	538,272.01
47600	NCASSR SAST	2,306,357.00	6/16/2004	12/30/2009	2,844,629.01
47730	SAST Phase II	593,648.28	4/20/2005	9/30/2007	3,438,277.29
53753	SEAL	375,051.26	6/21/2007	1/25/2008	3,813,328.55
54707	SAST Phase III	2,246,000.00	1/25/2008	9/30/2009	6,059,328.55
55506	SAIC SEAL Support	128,066.47	4/25/2008	1/25/2009	6,187,395.02
56031	MCTET	65,062.13	9/29/2008	9/30/2009	6,252,457.15
56662	SAST ICDW	285,132.63	5/1/2009	4/30/2010	6,537,589.78
57106	SAST Academy	97,087.00	5/1/2009	4/30/2010	6,634,676.78
58268	IA Range UCMC BD 10	968,707.00	10/17/2009	09/14/2010	7,509,676.78
Total investment for SAST development		7,509676.78			

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

Proudly Operated by Battelle *Since 1965*

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)
www.pnl.gov