Secure Information Sharing for Training and Testing Events

Mission readiness for agents, troops, and equipment is essential to warfighter and national security. Connecting training (live, virtual, and constructive - LVC) and testing environments in a real-world manner – across security boundaries – allows for more effective training activities and more efficient test events resulting in overall cost savings, a better trained warfighter and more thoroughly and quickly tested equipment. Training cost savings are realized through the ability to train multiple groups at the same time, be they different national agencies or multinational forces (for example, U.S. and Coalition). Testing cost savings are realized through earlier detection and correction of issues and errors. For example, an unclassified rail gun can be tested with a ship’s classified communications system before the gun is mounted on the ship and is deemed “classified” which reduces the potential for rework and improves implementation time.

**SIMSHIELD™**

SimShield™ is an accredited commercial-off-the-shelf [COTS] fixed-format data guard with the capability to label, segregate, protect, and exchange data between systems executing at different sensitivity or classification levels. SimShield meets the data format, near real-time performance and low latency requirements for distributed simulation operations, live training exercises, and test events.

In the LVC training environment, SimShield provides secure interoperability across networks at multiple classification levels, which
SimShield allows the most realistic and beneficial training exercises for U.S. and Coalition troops. The use of SimShield in these exercises enables training assets that operate under different security classification levels to fully communicate and securely interact, creating the most realistic training exercises possible.

In the Research, Development, Test & Evaluation (RDT&E) environment, SimShield allows tests on distributed components to be performed in near real-time and analyzed in a matter of hours. This drastically reduces testing cycle time, which provides large financial benefits. SimShield is listed on the U.S. Unified Cross Domain Management Office (UCDMO) Baseline list as an approved cross domain transfer solution. Because SimShield is an operationally accredited system, the Certification and Accreditation (C&A) process is streamlined for individual installations. SimShield consists of two components: the Policy Editor™ and the Trusted Bridge™ (Figure 1).

### POLICY EDITOR™

The Policy Editor is a stand-alone system on which security classification and domain experts build and review re-classification rules that govern the intercommunication between single level networks. The graphical user interface provides for human review and approval in addition to automated system checkpoints to ensure that the rule set is built accurately before being loaded into the Trusted Bridge.

- Supports security domain and data experts in defining classification filtering and sanitization rules between networks communicating through the Trusted Bridge;
- Provides persistent storage for rules and associated reclassification justifications, and;
- Provides an intuitive, user-friendly interface.

### TRUSTED BRIDGE™

Trusted Bridge, the SimShield guard component, provides the solution’s multilevel security and bi-directional filtering capabilities. The administrator installs and implements the approved Policy Editor rule set on the Trusted Bridge to check the data for type and content. The rule set enforces separate and distinct filter rules before passing, failing, or sanitizing (disguising) the data flowing from high to low and from low to high.

The Trusted Bridge provides a near real-time automated secure two-way data transfer between networks at different security levels in DIS, HLA or TENA environments. The most important challenge with two-way data transfer is ensuring that classified data is labeled, segregated, and protected to prevent the transfer and disclosure of classified information to a network that is not authorized to access the data.

### Data Types and Protocols

<table>
<thead>
<tr>
<th>DATA TYPE OR PROTOCOL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TENA LROM</td>
<td>Test and Training Enabling Architecture Logical Range Object Model Used for live training and testing environments.</td>
</tr>
<tr>
<td>HLA FOM</td>
<td>High Level Architecture Federated Object Model Provides the ability to interconnect two or more HLA Federations operating at different security classification levels.</td>
</tr>
<tr>
<td>DIS</td>
<td>Distributed Interactive Simulation Typically used for virtual training and simulation.</td>
</tr>
<tr>
<td>RTP</td>
<td>Real-Time Transport Protocol</td>
</tr>
<tr>
<td>MPEG2-TS</td>
<td>MPEG-2 Transport Stream</td>
</tr>
<tr>
<td>MPEG-PES, MPEG-PSI</td>
<td>MPEG Packetized Elementary Stream MPEG Program –Specific Information Stream</td>
</tr>
<tr>
<td>MPEG-Video, MPEG-Audio</td>
<td>MPEG Video and Audio Elementary Streams</td>
</tr>
<tr>
<td>KLV Metadata</td>
<td>Key-Length-Value</td>
</tr>
</tbody>
</table>

Table 1: Data Types and Protocols
ADMINISTRATION AND MANAGEMENT

Logging and Auditing
SimShield provides automatic logging within the Trusted Bridge for user and system activities. When enabled, Trusted Bridge logging is redirected to a remote syslog server at (and only at) the high side. This capability allows for central logging and archiving. Additionally, a logwatcher utility sends administrators email alert notifications and/or displays the alerts on-screen in real time.

Certification and Accreditation (C&A)
SimShield is engineered to satisfy cross domain security requirements for the Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI) C&A processes. RTCS products are installed and accredited in operational systems around the world.

CONCLUSION
Forcepoint™ develops the most secure, yet flexible, data sharing technologies for military, defense, intelligence, and civilian agencies throughout the U.S., Five-Eyes nations, and NATO member countries. SimShield provides a secure solution to the difficult problem of enabling secure and seamless training and testing across different security classifications. With the most enterprise-wide deployments throughout the world, our proven solutions deliver the right data, to the right people, at the right time to maximize efficiencies and reduce costs. Forcepoint also offers an experienced professional services team to guide customers through the technical implementation and C&A processes.


CONTACT
www.forcepoint.com/contact

ABOUT FORCEPOINT
SimShield, Policy Editor, and Trusted Bridge are trademarks of Forcepoint, LLC. Forcepoint™ Federal is a trademark of Forcepoint, LLC. SureView®, ThreatSeeker® and TRITON® are registered trademarks of Forcepoint, LLC. Raytheon is a registered trademark of Raytheon Company. All other trademarks and registered trademarks are property of their respective owners.