Current military operations and the joint vision of future warfare depend upon information systems that cannot be adequately secured with existing techniques. To address this urgent national problem, the Defense Advanced Research Projects Agency (DARPA) has created several research programs to further the science and technology of information assurance and survivability. The second DARPA Information Survivability Conference and Exposition (DISCEX II) event represents the culmination of the DARPA Information Assurance (IA) Program. DISCEX collects significant program results of many research efforts into a single archive. In doing so, the conference and proceedings facilitate technology transition by increasing visibility of these efforts to several groups. The audience not only includes a broader research community, but also the operational military, developers of military systems, and the commercial industry that generates “off the shelf” systems comprising most military information systems. DISCEX II also provides insight into interim progress of broader information assurance and survivability research investments at DARPA. The goal is to stimulate scientists, developers, and joint operational customers with research products, experimental results, and capabilities emerging from DARPA research to better address military needs for information security.

The early 1990’s witnessed exponential growth of attacks against military networks. In response to this growing threat, DARPA began an Information Security research program in 1994. Additional programs in High Confidence Networking and High Confidence Computing were funded in 1995. By 1998 the DARPA Information Survivability program additionally consisted of research into survivability of large-scale systems and wrappers for assuring legacy systems. Results of the Information Survivability program were presented at the first DISCEX conference on 25 – 27 January 2000.

DARPA initiated the Information Assurance program in December of 1996, recognizing that information security is a system wide problem requiring application of several technologies in concert. Drawing upon technologies being developed under the Information Survivability program, the IA program sought research in information assurance system architectures, integration, protection, advanced boundary controllers, malicious code detection, intrusion detection, monitoring, threat detection, incident response, recovery, automatic response, system integrity, vulnerability assessment, systems analysis, security management, risk management, and decision support. This breadth of research topics and an emerging process of scientific experimentation played important roles in debunking misleading lore and identifying effective novel strategies in previously unexplored research areas.

The growing importance of information assurance and the success of earlier programs provided a foundation for expansion of the information assurance investment at DARPA in 1999. This expansion created several new programs. These programs include Fault Tolerant Networks, Dynamic Coalitions, and Information Assurance Science & Engineering Tools, along with the precursors to Cyber Panel and Organically Assured & Survivable Information Systems. Interim results from many of these programs are presented here along with the results of the Information Assurance program.
**Information Assurance**

The grand hypothesis of the Information Assurance program was that trustworthy systems could be composed of less trustworthy components. Strategies for doing so included layering and dynamic defense leveraging and integrating prevention, detection, response, and security management technologies. Such integration requires a system perspective. By seeking principles of effective composition, the IA program began charting a path for safe and effective leverage of less trustworthy components. These less trustworthy components include the many commercial products used pervasively in military and critical infrastructure systems, and also include military specific systems designed under firm schedule and budget constraints not conducive to high assurance development. This breadth of perspective was crucial to lighting the path of investments to come.

**Cyber Panel**

Commanders need to know when the information systems and networks their operational functions depend upon are threatened or degraded by serious or large-scale cyber attacks. Their engineering and operations staffs need tools to help them determine and carry out effective responses for defending their systems. The Cyber Panel Program seeks to provide theater-level capabilities to help defend mission-critical information systems by monitoring them for signs of cyber attack, and allowing operators to manage the operation of system security and survivability technologies to avert or resist attack. Within two years, this program will deliver technologies that can be used to build such a monitoring and management system. The goal is to create and validate architectures, algorithms, techniques, and automated tools that aid identification of coordinated attacks, assessment of system health, mission impact assessment, course of action selection, and help carry out effective security and survivability posture changes, either proactively or in response to the appearance of attacks.

**Dynamic Coalitions (DC)**

The Dynamic Coalitions program is developing technology to enable secure collaboration within dynamically established mission-specific coalitions while minimizing potential threats from increased exposure or compromised partners. The technology products will support the secure creation of dynamic coalitions including the necessary technologies for policy management, group communications, supporting security infrastructure services, data sharing, and joint collaboration spaces. These areas are critical for future warfighting scenarios – both joint and multi-national.

**Fault Tolerant Networks (FTN)**

The Fault Tolerant Networks program is developing focused technologies that support continued network operation in the presence of successful attacks, particularly addressing vulnerabilities and issues expected to arise in DoD’s emerging network-centric warfare vision. The technologies developed by this program will leverage previous work in fault tolerant systems and apply these technologies to the networks of the future. This will reduce the amount of damage sustained during an attack and allow the networks to maintain an acceptable, minimum level of functionality. These include technologies for strengthening networks by introducing fault tolerance capabilities against possible attacks at the network level, emphasizing
integrity and availability; and technologies for mitigating potential vulnerabilities associated with denial of service attacks. Additionally, technologies that address attack response mechanisms, using active network technology, will allow the networks of the future to assist in their own protection and be more tolerant of future attacks.

**Organically Assured and Survivable Information Systems (OASIS)**

The Organically Assured and Survivable Information Systems Program seeks to provide defense capabilities against sophisticated adversaries to allow sustained operation of mission critical functions in the face of known and future cyber attacks against information systems. The technology development goals are to conceive, design, develop, implement, demonstrate and validate architectures, tools and techniques that would allow fielding of organically survivable systems. The technology products will include architectures for building intrusion tolerant systems from potentially vulnerable components; real-time execution monitors to detect malicious mobile code and prevent damage by and propagation of malicious code; error detection techniques and tolerance triggers; error compensation, error recovery, and error response technologies; and assessment and validation methodologies to evaluate intrusion tolerance mechanisms.

Collectively these programs comprise a significant portion of the information assurance and survivability research at DARPA from late 1999 through 2001.

**These Proceedings**

This publication represents the second DARPA Information Survivability Conference and Exposition (DISCEX II) proceedings and contains research papers describing projects in the areas of the information assurance and survivability programs described above. The sections of these proceedings are grouped by topic so similar research projects can be studied together. Contributions from 17 academic institutions, 46 industrial research laboratories, and three government research laboratories describe progress in research performed for information assurance and survivability. These proceedings have been peer reviewed, although not strictly in the traditional sense of a refereed conference or journal. Participating reviewers are noted in the Acknowledgments section.

We are confident these proceedings represent high quality papers describing the research conducted at each institution. We hope these proceedings will serve as a technology transfer vehicle for anyone interested in technology available today, conveying the many ideas and results from information assurance and survivability research at these institutions. We further hope the results presented here will provide an excellent source of ideas and insight for this rapidly expanding community, and catalyze discovery and application of new techniques for securing our nation’s information systems.

**World Wide Web**

Although the DARPA Information Assurance program has ended, current descriptions of activities within the information assurance and survivability programs are maintained with links to performers’ sites in the table below. These sites will provide the reader with opportunities for
contact and collaboration to accelerate the technology transfer process and the progress of research and development of survivable information systems.

<table>
<thead>
<tr>
<th>Information Assurance</th>
<th><a href="http://dtn.darpa.mil/iso/">http://dtn.darpa.mil/iso/</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Panel</td>
<td><a href="http://dtn.darpa.mil/iso/">http://dtn.darpa.mil/iso/</a></td>
</tr>
<tr>
<td>OASIS</td>
<td><a href="http://dtn.darpa.mil/iso/">http://dtn.darpa.mil/iso/</a></td>
</tr>
</tbody>
</table>

Jaynarayan Lala  
Douglas Maughan  
Catherine McCollum  
Brian Witten  
DARPA/ATO  
DARPA/ATO  
DARPA/ATO  
DARPA/ATO  
jlala@darpa.mil  
dmaughan@darpa.mil  
dmccollum@darpa.mil  
bwritten@darpa.mil

Arlington, Virginia
June 2001