



In a continuing effort to have information shared with our sponsors and among different parts of MITRE, I am pleased to launch this first issue of *The Edge*. As we all know, information technology advances at a rapid rate and we are obviously involved in nearly all aspects through our various project work programs as well as MITRE's research effort. I congratulate the I-Team and co-publishers Mark Maybury and Steve Huffman for this fine inaugural issue.

The Edge will report information technologies and applications that are strategic to the future of our country's national security. Technology topics include the Defense Information Infrastructure, information systems architectures, distributed interactive simulation, new information services, object technology, legacy system migration, and the year 2000 problem.

The Edge will report information technologies and applications that are strategic to the future of our country's national security. Technology topics include the Defense Information Infrastructure, information systems architectures, distributed interactive simulation, new information services, object technology, legacy system migration, and the year 2000 problem.

Vic DeMarines
President and CEO,
MITRE Corporation



Quickturn Integrates IT

by Daryl Morey

“**P**AN TO THE SARAJEVO AIRPORT USING MSIIA.”

Jeff: Lynette, I am looking at the airport. There are some transport planes there that could be used to transport SA's (Surface to Air missiles).

Lynette: Let me show you what I found. I'm putting a white-board called 'SA site' into the room. Why don't you bring it up? The image is a recent senior gaze image taken in the exclusion zone. This area is supposed to be inactive.

Jeff: [opens white-board] I've got it up.

Lynette: [circling vehicle on image] There is a vehicle here - something is going on.

Jeff: [circling confusing part of image] What are these?

Lynette: Hmmm... They look like SA-2 launchers.

Jeff: I agree, we should notify the J2.

The above is a transcript from a QuickTurn enabled scenario where Jeff and Lynette, intelligence analysts, work together to discover a newly active surface to air missile site.

QuickTurn is a collaborative environment system for multi-source intelligence analysis. A collaborative environment system is one that allows people to work together as if they were in the same room. Multi-source means that various sources of intelligence, like an imaging tool and document browser, are available in an integrated environment.

What is the motivation for building a system like QuickTurn? We can answer that question by looking at the current limitations of image analysis technology:

Continued on Page 2

In This Issue...

Quickturn

A collaborative environment system for multi-source intelligence analysis1

Predator

A spatio-temporal information system pilot for managing Bosnian Predator video3

OSIS

A MITRE-designed virtual private network for sharing open source information about Intelligence agencies and other organizations4

Year 2000 Problem

The end is near7

Collaborative Systems @Work

The QuickTurn system is designed for applications, such as air campaign planning, where it is necessary for many people to pool their knowledge and perspectives quickly to reach a workable plan.

Besides air campaign planning, there are many other areas in which a multi-source collaborative system like QuickTurn could be valuable:

- In a 911 call center...instead of operators consulting manuals for a procedure, they could quickly recall video with

instructions or collaborate with an expert in the problem area who is on call.

- In dispersed organizations...the ideal team could be assembled on every project through virtual workspaces without the limitations of geography.
- In a support organization...knowledge bases from the organization could be integrated with other vendors knowledge bases into an easily searched single source database for technical solutions.

If you have an application where you think a multi-source collaborative environment system would be beneficial,



please contact
Lynette Hirschmann
at 617-271-7789 or
lynette@mitre.org.



Intelligent Information Access presents Quick Turn—continued from page 1

- Important information and images reside on hard copy, not accessible from an analysts workstation.
- Collaboration and information sharing between analysts are difficult.
- Knowledge gained by the analyst is lost because there is no method for saving and recalling information between sessions.

The result of these limitations is slow image analysis sessions that repeat the mistakes of the past. The objective of the QuickTurn system is to overcome each of these limitations to achieve an order of magnitude increase in efficiency and quality of analysis.

QuickTurn tackles these problems by integrating three solutions produced by MITRE's Advanced Information Systems Center (AISC):

- MSIIA (Multi-Source Integration and Intelligence Analysis) - In itself a multi-source analysis tool, MSIIA provides quick and accurate access to current or past images, radar intelligence and

unmanned air vehicle video.

- FISH (Forager for the Information Super-Highway) - FISH is a multiple information source document browser with rapid visual drill down and filter capabilities. Reports generated by analysts are automatically made available for recall through FISH.
- CVW (Collaborate Virtual Workspace) - CVW provides the framework for data and application sharing, virtual video conference meetings and white board technology.

QuickTurn would obviously not be effective if it just threw these technologies together. Accessing multiple systems simultaneously can cause confusion and information overload for a user. QuickTurn addresses this problem with a Multimodal Interpreter that automatically takes input from various sources, such as the mouse, speech, keyboard, and gestures. It then routes this information to the proper sub-system. At the start of the SA scenario, Jeff told QuickTurn, "PAN TO THE SARAJEVO

AIRPORT USING MSIIA". The Multimodal Interpreter takes this spoken command, interprets it as a call to the MSIIA system and passes it to the Interface Router.

The Interface Router does exactly what its name implies. It routes commands and information to the proper integrated sub-system. While Jeff and Lynette were using the whiteboard technology to mark up the SA site image, the interface router ensured their commands were sent to the collaborate virtual workspace (CVW). The power of the Interface Router is that it is designed for easy integration with any future technologies that may need to be added.

A prototype of the QuickTurn system has been built and demonstrated to DARPA.

To find out more information or request a demo, please contact
Rod Holland
at 617-271-7427 or
rholland@mitre.org.



MSIIA Hunts Predator in Bosnia

by Steven Hansen

“We’ve been hit.”

With those three words, a 40-minute test of wills and technical acumen began for MSIIA operators in Bosnia.

The MSIIA (Multi-Source Intelligence Integration and Analysis) system is an information fusion system that allows analysts to quickly view multiple streams of visual data. MSIIA is currently being used to support the Predator Unmanned Air Vehicle (UAV) operations in Bosnia for the Combined Air Operations Center in Vicenza, Italy.

The call for help came at 09:49 ZULU on 10/1/96 from the Predator UAV pilot in Tazar, Hungary. The pilot reported that the vehicle was still in the air, but he had lost the video feed, oil pressure and telemetry data. Because the video feed was lost, MSIIA was used to find the vehicle’s location by retrieving geo-registered digital videos from the previous ten minutes of flight. Once the location was determined, MSIIA was used to examine past image data in the area to get an indication if the vehicle was actually fired upon. The flight area was in the area of Jusiki, a contested mountain village where Muslim civilians were attempting to move back into their homes. The village is about 40 km E of Tuzla. Initial analysis on MSIIA revealed several roadblocks around the village manned with APCs (Armored Personnel Carriers) and medium duty trucks. There were antenna whips and individuals lightly armed, but no evidence of fire on Predator. MSIIA’s evidence that Predator was not fired upon was confirmed when, four minutes after the initial distress call, the video feed and telemetry data was brought back on-line.

The aircraft was gliding at a sink rate of approximately 500 feet per minute and heading back home NW,

attempting to drift as far as possible over the zone of separation. It soon became obvious that the vehicle would have to ditch; the question now was where. A quick calculation using the sink rate, altitude, and heading produced a gross estimate of a 1 x 5 km impact area approximately 25 km northeast of Tuzla.

MSIIA was then used to pull geo-registered Eagle Vision and CIB (Controlled Image Base) satellite imagery from its database of the predicted impact sites. Others in the ISARC (Intelligence Surveillance and Reconnaissance Cell) pulled 1:50 scale paper maps of the area. There was confusion about the nature of the probable impact zone since the paper 1:50 maps were considerably different from the satellite based imagery in MSIIA. The difference turned out to be inaccuracies due to the age of the paper maps. For example, a marginally distinguishable mine symbol on the map turned out to be a strip mine that had grown to several square kilometers over the years since the map was created. There were also several new roads in the area supporting the strip mine.

Every effort was being made to divert the vehicle away from populated areas while maintaining accessibility for recovery. Prediction of the probable crash site was enhanced because the video feed from the vehicle



remained live through the crash (in fact the video transmission survived the crash!) With the live video from MSIIA, analysts were able to track the flight path of the vehicle and aim the EO (Electronic Optical) sensor. Information on the optimal ditch site was then fed back to the pilot. At 10:12 ZULU (23 minutes from the initial loss of engine and signal) the vehicle bellied in, losing one wing but remained surprisingly intact.



A Navy P-3 was then vectored to the site while a helicopter team (Russian!) was scrambled from Tuzla in order to secure the site. Later that afternoon, the vehicle was transferred back to Tuzla where it was determined that there was no sign of externally inflicted damage. In fact, thanks to the MSIIA system and the quick thinking of everyone involved, the Predator vehicle was repaired and back in operation for its next scheduled mission.

To find out more information about MSIIA, please contact **Steven Hansen** at 617-271-7326 or swh@mitre.org.



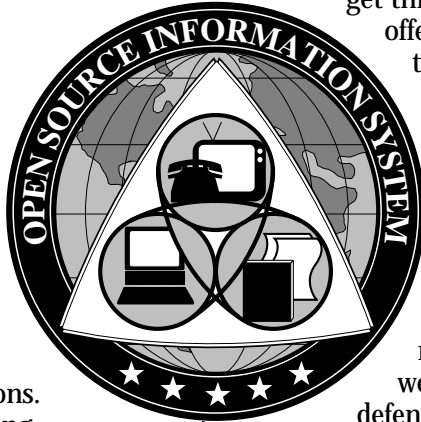
HOW DEEP IS THE OSIS? *by Walt Lazear*

INTRODUCTION

The Open Source Information System (OSIS) is an electronic network for accessing and sharing unclassified and open source information and value added services among Intelligence

Community agencies and related organizations. MITRE has been working with the Community Open Source Program Office (COSPO) for over three years to design and field OSIS. The team has been composed of members from four MITRE technical centers: the Networking Technical Center, the Security Technical Center, the Advanced Information systems Center, and the Open Systems Center. We discovered that no technical center had all the answers, and it indeed took the work and knowledge of those four centers to come up with an integrated solution.

What is open source information? Open source information is any unclassified information, in any medium, that is generally available to the public, even if its distribution is limited. It includes but is not limited to the traditional "gray literature" of conference proceedings, technical reports, etc. Television documentaries and other programs, commercial CD-ROM products, newspapers, maps, journals, advertising brochures, magazines and the Internet's vast holdings are all open source information resources.



get through OSIS? OSIS offers on-line access to the unclassified information resources of participating US Government agencies. For example, Janes Electronic Library of 24 titles provides up-to-date information on military equipment, weapons systems, and defense products worldwide. The CIRC Database (Central Information Reference and Control) is a database of over 10 million titles on scientific and technical topics, including patents, standards, military equipment and systems. The Conference Database is a source of upcoming symposia, congresses, conventions, etc., in the areas of science, technology, engineering, politics, and economics.



IC ROSE is a database service providing searchable text articles from hundreds of periodicals on a wide range of subjects. FBIS (Foreign Broadcast Information Service) products are on-line, including the Daily Reports, Science & Technology Perspectives, Trends, and Pacific Rim Economic Review. The TEL (Technical Equipment List) is an electronic index to over 100,000 brochures and manuals on telecommunications and related equipment. The TCOM (Telecommunications) database contains abstracts and complete articles on telecommunications related topics. The Defense Mapping Agency's DTED (Digital Terrain Elevation Data) is the on-line map

collection providing worldwide coverage (you should see their 500 CD-ROM jukebox!). Additionally, commercial datasources such as Oxford Analytica have been purchased for intelligence community use and reside on OSIS. There are also unclassified library holdings of several OSIS member agencies, including Defense Intelligence Agency, on OSIS. In addition to open source information, OSIS offers specialized software and other tools to assist users in analytical and graphical interpretations of data.

For example, OSIS currently makes available the National Air Intelligence Center's (NAIC) SYSTRAN[®] machine translation (MT) capability to provide "real time" rough translations of foreign language information. MITRE's creation of a World Wide Web (WWW) front-end for MT allows the inclusion of information directly from WWW sites (see our example of this capability in the next section).



Language training materials and courseware from the Center for Advancement of Language Learning (CALL) are available on OSIS. Through "hot links", OSIS will connect users directly to key additional Federal open source resources, such as the DTIC (Defense Technical Information Center) and the NTIS



OSIS RESOURCES

What kinds of open source information can authorized users



(National Technical Information Service), each of which offers unique open source databases and other products and services. At the end of 1996, users had access to more than thirty open source information products and tools via OSIS.

So much for “finished” intelligence products and tools. OSIS also provides its users with direct, yet protected, access to the Internet and its broad range of worldwide open source information resources. For common Internet applications (Web Browsers, Net News readers, telnet and FTP), OSIS uses proxies. Since these proxies give seamless access to the Internet, there is no difference to the user between surfing OSIS and surfing the Internet.

AN APPLICATION OF OSIS

Let's look at a prime example of the power of combining OSIS tools and the Internet access. Remember the OSIS machine translation tool? Well, here's how to use it with the World Wide Web: the OSIS user surfs the Internet to find a foreign language magazine or newspaper online with headlines that are Web links. Our example shows a German online magazine “*Journal für Deutschland*”.

The user copies the Universal Resource Locator (URL) for the paper, brings up the NAIC MT page, and pastes in the URL. Note that you could paste in paragraphs of free text instead of Web references.

You hit the Translate button, and shortly thereafter you are looking at an English version of the newspaper page with intact URLs that you can click on to progress further!

OK, so it's not Shakespeare, but you can tell what the stories are about. Also, note that only text is translated; web logos and graphics are left unchanged. Hyperlinks are preserved.

Continued on Page 6



Ein Magazin des Presse- und Informationsamtes der Bundesregierung

Das Magazin ist Teil der Öffentlichkeitsarbeit der Bundesregierung. Es wird von *germany.net* in eigener Verantwortung im Internet verbreitet. Die Texte sind frei verwendbar, wenn sie unverändert übernommen werden und ein Hinweis auf die Quelle (Presse- und Informationsamt der Bundesregierung) erfolgt. Durch die Digitalisierung des Textes kann es zu Fehlern kommen. Der verbindliche Text kann beim Presse- und Informationsamt der Bundesregierung, D-53105 Bonn, angefordert werden. Die Bilder dürfen nur nach vorheriger Anfrage weiterverwendet werden.

- [Berlin ist unsere Chance](#)
- [Starke Frauen braucht das Land](#)
- [Kinder, Kinder](#)
- [Mit Tempo voran](#)
- [5 Jahre Demokratie, ein Theologe zieht Bilanz](#)
- [Dünen können wieder grünen](#)

German to English

This system was acquired by NAIC in 1983 and has undergone significant development. It now has the largest stem dictionary of all systems - 226,380 words.

1. Type or paste the text or URL of document to translate

For examples of text documents and URL samplers, click [here](#)

http://www.journal.de

Systran German Input. Type character-for-character; for special characters use the following transliteration:

ä - ae ö - oe ü - ue ß - ss

2. Change options below first if needed then click on

How Deep Is The OSIS?—continued from page 5



A magazine of the pressing and office for information of the Federal Government

The magazine is part of the public work of the Federal Government. It becomes of *germany.net* within own responsibility in the Internet spread. The texts are freely usable, if them invariably are taken over and a reference to the source (pressing and office for information of the Federal Government) takes place. By the digitization the text can it to failures come. The obligatory text can with Pressing and office for information of the Federal Government, D53105 Bonn, are called. The pictures may only after previous inquiry are re-used.

- [Berlin is our chance](#)
- [The country needs strong women](#)
- [Children, children](#)
- [With speed in front](#)
- [5 years democracy, a theologian balance draws](#)
- [Dunes kuennen again become green](#)

OSIS BEHIND THE SCENES

If we back up a bit and look behind the scenes, just what is OSIS?

- To the Network Technical Center, it is a communication infrastructure with routing plans, split Domain Name Service, proven technology, and strong management.
- To the Security Technical Center, it is an enclave of restricted-access information that is protected by a security policy, risk assessment, and application firewalls.
- To the Open Systems Center and Advanced Information Systems Center, it is a client-server system of information repositories and advanced information services and tools accessed through a common Web-based user interface.

Each view of OSIS has multiple dimensions, numerous technologies, and diverse methodologies. The combined strengths of the technical centers made possible the deployment of OSIS in less than two years. Along the way, a fundamental cultural

change occurred towards Internet access and towards cooperation among the participating intelligence agencies. While two is a large number in computer years, these socio-political changes take real time. Now we accept Internet access, Web browsing, and security firewalls as the norm. In 1993, these were fledgling technologies with many associated uncertainties and threats.

Early in the project, the focus was on defining and creating infrastructure (connectivity, networks, firewalls, servers, and community self-help). The MITRE team led the efforts in technical development, component prototyping, and administrator training for the first 16 OSIS sites. New technologies are still being added to the firewalls. The most recent example is a current effort to support the Defense Message System with its X.400 messaging and X.500 directory services.

Once a stable and secure network was in place, the focus changed to address the usability of OSIS. An enhanced design for an Intelligence Community unclassified intranet was defined and implemented that improved usability and further opened communication among the agencies. Today, OSIS accounts are a popular commodity. New sites are being added, dial-in facilities are expanding, and OSIS is available from the European Theater to the Pacific Rim. During 1997, two MITRE-developed proof-of-concept

capabilities will be piloted on OSIS. One is the Open source Research Network (OSRN), which allows OSIS analytic users to register open source information needs and obtain responses. The other is the Broadcast News Navigator (BNN), which enables users to browse current and past broadcast news stories by viewing video and closed-caption text. The latter of these capabilities is based on MITRE Sponsored Research multimedia initiatives.

The focus has continued to shift and now is clearly set on expanding the information content available through OSIS. Discussions with potential producers of open source information are occurring daily. We eagerly await the new offerings they will bring. In addition, OSIS may expand beyond United States agencies. Work is underway at MITRE to facilitate the internationalization of OSIS.

CONCLUSION

A running joke within the Intelligence Community is that to Intelink (the classified intelligence web), OSIS is Intelink-U (for unclassified). But on the COSPO side of this friendly rivalry, Intelink is known as OSIS-S (for secret). Although OSIS does offer 1-800 dial-in access, and although it faces a different threat than Intelink does, it can still leverage lessons learned from Intelink (such as getting user-helpful search facilities in place early). The point is that OSIS is many things to many people because it has a rich infrastructure, a set of problem solutions, and a growth potential as boundless as the Internet it accesses.

To find out more information about OSIS, please contact **Walter Lazear** at 703-883-6515 or lazear@mitre.org.



Year 2000 Problem *By Robert A. Martin*

If not addressed, the coming of the year 2000 will draw a dark and chaotic cybernetic shadow across our national and international computer-based society and the information technology on which it runs. Behind the apparent simplicity and innocence of the calendar year moving from 1999 to 2000 is hiding an amorphous, multi-tentacled menace that will affect most systems, including those critical to the banking world and our nation's defense. Devices for processing credit cards, which are used by merchants worldwide, cannot yet handle expiration dates beyond 1999. In early tests of our missile warning systems for date problems, a year 2000 glitch stopped it cold at the simulated time of 23:59:59 on December 31, 1999. While this glitch has been found and is being fixed, other problems still await our attention.

As the year 2000 approaches, the problems associated with the date roll-over in command and control computer systems have become more apparent. The practice of representing year dates with two digits brings into question the stability and reliability of our national military and air space management computer systems as well as the majority of other systems our government and industries rely upon to carry out their work.

In the past, for efficiency of storage space, most hardware manufacturers and computer programmers omitted the first two digits of the year (i.e., century) when referring to dates in their programs. This programming convention created an environment that has become known as the Year 2000 (Y2K) problem.

When these dates are built into an algorithm or decision process, problems will arise once the date rolls over from 1999 (99) to 2000 (00). They include the inability of sort rou-

tines to perform properly, the reversal of logic decisions, the inability of inventory systems to generate correct stock level reports, the inversion of security access rules, and the inability to properly validate intelligence data.

There are three other date related issues that compound the problem:

- Many systems fail to take into account that the year 2000 is a leap year.
- Many systems assign special meaning to specific values of date fields or hard-code values in the software.
- Many systems define and use a date data type that will roll over and fail due to a dependence on a specific storage structure.

The failure to process the dates properly from any of these causes could lead to catastrophic failures in our weapon systems. In addition, most systems deal with a range of dates both before and after the present date. This window of time is different for different types of systems and forces analysts to test many situations beyond the Year 2000. On top of all this, testing (either to find the problems or verify the fixes worked) is not easily accomplished with our normal test approaches and facilities.

System engineers at MITRE are applying their expertise in systems and software to assist programs in moving through the five stages of dealing with the Y2K problem:

- awareness
- assessment (finding the problem)
- renovation (making the changes)
- validation (testing the solutions)
- implementation (fielding the fixes)

Military and air space management applications require additional care and consideration in meeting the Y2K problem due to their extensive interdependencies, older infrastructures, and use of legacy languages. Three informational briefings on the



Y2K problem have been presented by MITRE to many different DOD and software industry public forums, including software technologies conferences and Year 2000 conferences. One of these briefings addresses the assessment of the effects of the Y2K problem; the second briefing discusses the appropriate roles for tools in addressing the Y2K problem; and the third discusses management and reporting ideas to help conduct Y2K resolution efforts.

MITRE, in coordination with the Office of the Secretary of Defense (OSD), the Defense Information Systems Agency (DISA) and the Electronic Systems Center (ESC), has established a Y2K web-site to help organizations find the information they need to successfully address their own Y2K problem. The web site contains:

- briefings
- methods for costing the Y2K problem
- useful links to other Y2K resources
- an online catalog containing information on Y2K tools, services and consultants
- information on the ability of commercial hardware and software to handle specific Y2K problems, such as leap year issues
- a collection of solutions to the various Y2K problems our sponsors encounter that includes examples, source code, and lessons-learned

Continued on Page 8

Year 2000 Problem—continued from page 7

System Name	Risk Summary		Sources of Risk					Implementation Status				
	Mission Criticality	Solution Risk	Tech Risk	Funding	Resource People Facilities Supp Cont	Time	Assessment	Renovation	Validation	Implement	Date Done	
CLOSE1	Red	Yellow	Green	Green	Green	Green	Green	Yellow	White	White	1998	
OTHER1	Yellow	Red	Red	Yellow	Green	Green	Red	Red	Green	Red	1997	

The Y2K web-site is located at <http://www.mitre.org/research/y2k>
 For those on MITRE's internal MII, the address is <http://www-i.mitre.org/research/y2k>
 MITRE is also conducting research and experimentation to evaluate the technology issues relevant to analyzing and fixing Y2K problems in the Government's military and air space management systems. These directed research and risk mitigation efforts are investigating the potential payoff in extending and enhancing in-house and commercial reverse-engineering based Y2K analysis tools and the potential benefits of adjuncts to compilers that would allow for correct 2-digit date usage.
 The results from these proof-of-concept and risk mitigation investigations will be placed in the public domain for incorporation into commercially supported compilers and tools and will be disseminated through the MITRE Y2K Internet Web site.

Due to the severe schedule constraints (the end date can not be

changed) and budget limitations (no new monies are available to address this situation), senior management must be proactive in the oversight of these efforts. Senior management must also have current status information to allow them to make timely decisions to address any resource, priority, or trade-off questions as they surface. To this end, MITRE has developed a color coded "triage" scorecard specifically to: (1) enable the tracking of risk during the resolution process, (2) provide insight about resource status as resolution efforts proceed, and (3) to explicitly identify systems that are critical. The sample two entry scorecard shows both a critical and a non-critical system, each having various issues and risks.

The majority of our sponsors are using this Scorecard (in conjunction with lower level, detailed status information) to assess both the systems being developed for end-users and the facilities used to develop, test, and support these systems. The Y2K Triage Scorecard is a management

tool for providing periodic reports on the risk that Y2K problems will harm the missions of our DOD and FAA customers

MITRE's Y2K web-site is recommended by the DOD's Software Technology Information Clearing House and the Defense Technology Information Center's (DTIC) Data & Analysis Center for Software (DACS) as the most comprehensive Y2K site. The site is their recommended starting point for people or organizations looking to become familiar with the Y2K problem. MITRE is also heavily quoted and referenced on the Y2K topic by the press, including Government Computer News, Federal Computer Week, AFCEA's SIGNAL Magazine, and CIO Magazine. While much of our guidance and suggestions appear on the Y2K web site, additional help and support is available directly for those customers that require it.

To find out more information, please contact **Robert A. Martin** at 617-271-3001 or ramartin@mitre.org



The EDGE

MP 970000040-01

The Edge is published four times a year by the MITRE Corporation.

The MITRE Corporation
 202 Burlington Road,
 Bedford, MA 01730-1420

1820 Dolley Madison Boulevard,
 McLean, VA 22102

Daryl Morey, *Editor*
 Regina Hansen, *Editor*
 Richard Wilmer, *Editor*
 Pierre Nelson, *Designer*

For newsletter feedback or submission information, contact:

Daryl Morey, *Editor*
 Mail Stop: K308
 Telephone: (617) 271-2845
 E-mail: dmorey@mitre.org