



MIT Supporting Teams

- Can be named from any supporting center or project organization as needed, examples are payloads/cargo, solid rocket booster, flight operations and networks, etc.
- For STS-107 a Rapid Response Team is supporting the MIT in the field.



STS-107 Standing Interagency Independent Investigation Board

The independent board (named by Mr. O'Keefe as the Columbia Accident Investigation Board - CAIB) consists of a chair and seven members, supported by Headquarters, NASA Field Centers, and technical consultants, as required. Board Membership is as follows:

Chair: Adm (ret) Harold Gehman Jr. (Washington D.C.)

1. Maj. Gen. Kenneth W. Hess, USAF Chief of Safety (Kirtland AFB, NM)
2. Mr. Steven B. Wallace, FAA Director of Accident Investigation (Washington, DC)
3. Maj. Gen. John L. Barry, Director Plans and Programs, Air Force Materiel Command, (Wright-Patterson AFB, CA)
4. Rear Adm. Stephen Turcotte, Commander, Naval Safety Center (Norfolk, VA)
5. Dr. James N. Hallock, DOT Chief of Aviation Safety Division (Cambridge, MA)
6. Brig-Gen Duane Deal, Commander 21st Space Wing (Peterson AFB, CO)
7. Mr. G. Scott Hubbard, Director, Ames Research Center (Moffett Field, CA)

Executive Secretary: NASA Chief Engineer, Mr. Theron M. Bradley Jr. (NASA Headquarters, Washington, DC)

Ex-officio member: Mr. Bryan O'Connor NASA Associate Administrator, Office of Safety and Mission Assurance (NASA Headquarters, Washington, DC)



Mission Success Starts With Safety

Other Supporting teams to the CAIB

Independently assesses data and may conduct their own inquiries, tests, and actions.

Columbia Accident Investigation Board (CAIB)

(CAIB)

Independent Board

NASA Led
 Flight Crew Operations
 Mission Operations
 Engineering
 System Integration
 Payloads & Cargo
 MSFC Projects
 Space & Life Sciences
 Prime Contractors

Coordination

FEMA
 Homeland Security
 EPA
 DDMS
 NTSB
 FBI
 FAA
 Texas National Guard
 Local Law Enforcement
 U. S. Forest Service
 Other agencies

Headquarters Contingency Action Team

Mishap Response Team

Membership: Mission Management Team (MMT)

Mishap Investigation Team

Rapid Response Team

Orbiter

Emergency Operations Center

KSC Ground Operations

Data & Record Handling Team

External Tank
 Solid Rocket Booster
 Reusable Solid Rocket Motor
 Space Shuttle Main Engine



Mission Success Starts With Safety

Back-Up Slides



Key Definitions

- **NASA Mishap** - Any unplanned event that results in injury to non NASA personnel caused by NASA operations; damage to public or private property.. caused by NASA operations; occupational injury or illness to NASA personnel; damage to NASA property caused by NASA operations...or mission failure.
- **Type A Mishap** - A mishap causing death and/or damage to equipment or property equal to or greater than \$1 million. Mishaps resulting in damage to aircraft, space hardware, or ground support equipment that meet these criteria are included, as are test failures in which the damage was unexpected or unanticipated.
- **NASA Mishap Investigation Board** - A NASA-sponsored board, consisting of a single individual or a group of individuals with expertise in the area under investigation, which is appointed to investigate a NASA Mishap. Board members must not have any vested interest in the outcome of the investigation. Board members may be selected from NASA or other Government agencies. Observers may be obtained from these same sources or from non-Government sources, such as consultants.



Key Definitions

- **Mission Failure.** A mishap of whatever intrinsic severity that, in the judgment of the Enterprise Associate Administrator and the Associate Administrator for Safety and Mission Assurance, prevents the achievement of primary NASA mission objectives as described in the mission operations report or equivalent document.
- **Appointing Official.** The official authorized to appoint the mishap investigation board, mishap investigator, medical board, Center-level investigation, or technical investigation team to investigate a mishap or close call, or to accept the investigation of another authority. This official is also authorized to accept the final mishap investigation report, direct the responsible organization to develop a Corrective Action Plan (CAP), accept the CAP, track and close corrective actions, and produce a summary report of mishap-related activities upon completion.
- **Approving Official.** The official with the final responsibility to review and accept the NASA mishap investigation report as complete and in conformance with NASA policy.



Key Definitions

- **Finding.** A conclusion based on facts established during the investigation by the investigating authority.
- **Recommendation.** An action developed by the investigation board to correct the cause or a deficiency identified during the investigation. The recommendations may be used in the preparation of the corrective action plan.
- **Corrective Actions.** Changes to design processes, work instructions, workmanship practices, training, inspections, tests, procedures, specifications, drawings, tools, equipment, facilities, resources, or material that result in preventing, minimizing, or limiting the potential for recurrence of a mishap.



Key Definitions

Proximate Cause(s) – The event(s) and condition that occurred immediately before the undesired outcome, directly caused its occurrence, and if eliminated, or modified, would have prevented the undesirable outcome.

Root Cause(s) – One of multiple organizational factors that contributed to / created the proximate cause and subsequent undesirable outcome, and if eliminated or modified would have prevented the undesirable outcome.

Contributing Factor – A condition or event that may have contributed to the occurrence of an undesired outcome but if eliminated or modified would NOT by itself prevent the recurrence.

Significant Observation – A factor, event, or circumstance identified during the investigation that did not contribute to the mishap or close call, but if left uncorrected has the potential to cause a mishap, injury, or increase the severity should a mishap occur.



NASA Strategy for Staffing MIB

- **Type A Mishaps (death and/or damage, including mission failure equal to or exceeding \$1M or selected high-visibility cases):**
 - Administrator (or AA, Code Q) assigns a Board for the investigation
or
 - Enterprise Associate Administrator (EAA) assigns a Board
 - Members require AA Code Q concurrence to assure technical capability and independence.
- **Type B Mishaps (personal disability or damage greater than \$250K but less than \$1M) and lesser mishaps – the Center Director or program executive will form the board.**



Mission Success Starts With Safety

Overview of NASA Mishap Investigation Policy and Process and Contingency Planning

February 4, 2003

Jim Lloyd
NASA Headquarters
Office of Safety and Mission Assurance



Mission Success Starts With Safety

Purpose

- **To provide a top level overview of NASA Mishap Policies and Procedures and their connection to the ongoing contingency efforts for the STS-107 mishap**



NASA Policy and Procedures

- NASA has policy and contingency planning in place to assure the proper investigation of all mishaps (including Space Shuttle)
 - NASA Policy Document (NPD) 8621.1, "NASA Mishap Reporting, Recordkeeping and Investigating Policy," October 02, 2002.
 - NASA Procedures and Guidelines (NPG) 8621.1, "Procedures and Guidelines for Mishap Reporting, Investigating, and Recordkeeping," June 2, 2000.
- Policy may be downloaded from:
<http://www.hq.nasa.gov/office/codeq/doctree/doctreeec.htm>



Mission Success Starts With Safety
NPD 8621.1G Mishap Reporting, Investigating, and Recordkeeping Policy"

Office of Prime Responsibility : **Office of Safety and Mission Assurance (Code Q)**
Bryan O'Connor,
Associate Administrator

- Establishes NASA-wide policy for mishap reporting and investigating—signed by the Administrator.
- Describes purposes of mishap investigation, board appointment authorities, roles of responsible officials, and responsibilities for final report acceptance and approval.
- Requires all levels to have mishap response plans; e.g., pre-mishap plans, contingency plans, for response to emergencies.



Mission Success Starts With Safety

NPG 8621.1G, "NASA Procedures and Guidelines for Mishap Reporting, Investigating and Recordkeeping"

Office of Prime Responsibility : Office of Safety and Mission Assurance (Code Q)

**Bryan O'Connor,
Associate Administrator**

- **Establishes NASA-wide procedures and guidelines for mishap reporting, investigating and recordkeeping**
- **Provides definitions of types of mishaps, descriptions of reporting procedures, investigative techniques, report format, report timelines, report approval process, corrective action process, and lessons learned process.**

X-Sender: jmullin@mail.hq.nasa.gov

X-Mailer: QUALCOMM Windows Eudora Version 4.3.2

Date: Sat, 15 Feb 2003 13:48:31 -0500

To: a.h.phillips@larc.nasa.gov, aodonogh@hq.nasa.gov, alee@hq.nasa.gov,
bdolci@arc.nasa.gov, cathy.miller@msfc.nasa.gov,
tsabikos.a.papadimitris.1@gsfc.nasa.gov, chunt@mail.arc.nasa.gov,
clyde.dease@ssc.nasa.gov, dhall@wstf.nasa.gov,
Eric.G.Fuller@jpl.nasa.gov, Ezra.R.Abrahamy@jpl.nasa.gov,
frederick.w.battle.jr@jpl.nasa.gov, h.w.beazley@larc.nasa.gov,
jack_vechil@mail.dfrc.nasa.gov, dennis.g.perrin1@jsc.nasa.gov,
luequestion.wilkins@grc.nasa.gov, lengelbert@mail.arc.nasa.gov,
michael.moore@maf.nasa.gov, probles@nmo.jpl.nasa.gov,
sonja.alexander@hq.nasa.gov, stephen.a.turner@maf.nasa.gov,
terry.m.potterton.1@gsfc.nasa.gov, tom.ambrose@dfrc.nasa.gov,
wayne.kee-1@ksc.nasa.gov, Robert.Turner@hq.nasa.gov,
howard.kass@hq.nasa.gov, alee@hq.nasa.gov,
william.barry-1@ksc.nasa.gov, odomingu@hq.nasa.gov,
Catherine.Angotti@hq.nasa.gov, mmcneill@mail.hq.nasa.gov,
tspagnuo@pop200.gsfc.nasa.gov, Patrick.A.Hancock.1@gsfc.nasa.gov,
Jim.Carter@msfc.nasa.gov, Edwin.Jones@msfc.nasa.gov,
john.rogers@hq.nasa.gov, bnotley@mail.arc.nasa.gov,
gregory.l.ellis.1@gsfc.nasa.gov, t.f.middleton@larc.nasa.gov,
william.c.roeh1@jsc.nasa.gov, phillip.j.nessler.1@gsfc.nasa.gov,
pete.allen@msfc.nasa.gov, jlabrecq@hq.nasa.gov, cherbert@hq.nasa.gov,
astowes@hq.nasa.gov, Ernest.M.Graham@msfc.nasa.gov,
dan.thomas@hq.nasa.gov, g.m.watson@larc.nasa.gov,
rdilustr@mail.hq.nasa.gov, hstewart@hq.nasa.gov, speyton@hq.nasa.gov,
jlemke@hq.nasa.gov, whill@hq.nasa.gov, michael.stevens-2@ksc.nasa.gov,
jllloyd@hq.nasa.gov, prichard@hq.nasa.gov,
robert.t.gaffney1@jsc.nasa.gov, james.o.cheek@usago.ksc.nasa.gov,
guy.camomilli-1@ksc.nasa.gov

From: "Jonathan B. Mullin" <jmullin@hq.nasa.gov>

Subject: Fwd: NASA SEEKS HELP FROM SKY WATCHERS

The enclosed request for **Sky Watcher** data may be redundant, if is not, please distribute to your center and appropriate authorities. Regards, Jon

Mailing-List: contact ksc-news_release-help@kscnews.ksc.nasa.gov; run by ezmlm

X-No-Archive: yes

list-help: <mailto:ksc-news_release-help@kscnews.ksc.nasa.gov>

list-unsubscribe: <mailto:ksc-news_release-unsubscribe@kscnews.ksc.nasa.gov>

list-post: <mailto:ksc-news_release@kscnews.ksc.nasa.gov>

Delivered-To: mailing list ksc-news_release@kscnews.ksc.nasa.gov

Delivered-To: moderator for ksc-news_release@kscnews.ksc.nasa.gov

From: "Buckingham-1, Bruce" <Bruce.Buckingham-1@nasa.gov>

To: "1 'ksc-news_release@kscnews.ksc.nasa.gov' (E-mail)" <ksc-news_release@kscnews.ksc.nasa.gov>

Subject: NASA SEEKS HELP FROM SKY WATCHERS

Date: Fri, 14 Feb 2003 09:51:10 -0500

X-Mailer: Internet Mail Service (5.5.2653.19)

Allard Beutel
Headquarters, Washington
(Phone: 202/358-0951)

Feb. 13, 2003

Kylie Moritz
Johnson Space Center, Houston
(Phone: 281/483-5111)

NOTE TO EDITORS: n03-017

NASA SEEKS HELP FROM SKY WATCHERS

NASA is still seeking help from the American public to supply video and still images of the Space Shuttle Columbia on its return flight to Earth. There has been a great public response, but more material will help the investigation of the Columbia accident.

Columbia glided across the western U.S. just before sunrise Saturday, February 1. The Shuttle flew just north of San Francisco around 6:50 a.m. PST and broke up over eastern Texas around 8:00 a.m. CST. Any imagery, especially video, of the Shuttle's path might aid the Columbia Accident Investigation Board in determining the cause of the accident.

Media and private citizens who have video or still images of Columbia's entry path are encouraged to send it to investigators. Videotapes and photos will not be returned. For more information call:

Johnson Space Center Emergency Operations Center
(Phone: 281/483-3388)

Mail videotapes to:

NASA Johnson Space Center
Mail Code JA17
2101 NASA Road 1
Houston, Texas 77058

Email digital images to: columbiainages@nasa.gov

-end-

For automatic email subscriptions to this KSC originated press releases, send an Internet

Jonathan B. Mullin, 01:48 PM 2/15/2003 -0500, Fwd: NASA SEEKS HELP FROM SKY WATCHERS

electronic mail message to mailto:ksc-news_release-subscribe@kscnews.ksc.nasa.gov. With no subject or message. The system will reply with a confirmation via e-mail of each subscription.

To remove your name from the list at any time, send an email addressed to mailto:ksc-news_release-unsubscribe@kscnews.ksc.nasa.gov . With no subject or message.

or you can (un)subscribe on the World Wide Web at: <http://kscnews.ksc.nasa.gov/>

Status reports and other NASA publications are available on the World Wide Web at: <http://www-pao.ksc.nasa.gov/kscpao/kscpao.htm> .

Jonathan B. Mullin
Manager Operational Safety
Emergency Preparedness Coordinator
Headquarters National Aeronautics and Space Administration
Phone (202) 358-0589
FAX (202) 358-3104
"Mission Success Starts with Safety"

X-Sender: jmullin@mail.hq.nasa.gov
X-Mailer: QUALCOMM Windows Eudora Version 4.3.2
Date: Tue, 25 Feb 2003 07:30:07 -0500
To: hcat@hq.nasa.gov
From: "Jonathan B. Mullin" <jmullin@hq.nasa.gov>
Subject: Fwd: FW: Status Briefing
Cc: a.h.phillips@larc.nasa.gov, adonogh@hq.nasa.gov, alee@hq.nasa.gov, bdolci@arc.nasa.gov, cathy.miller@msfc.nasa.gov, tsabikos.a.papadimitris.1@gsc.nasa.gov, chunt@mail.arc.nasa.gov, clyde.dease@ssc.nasa.gov, dhall@wstf.nasa.gov, Eric.G.Fuller@jpl.nasa.gov, Ezra.R.Abrahamy@jpl.nasa.gov, frederick.w.battle.jr@jpl.nasa.gov, h.w.beazley@larc.nasa.gov, jack_vehil@mail.dfrc.nasa.gov, dennis.g.perrin1@jsc.nasa.gov, luequention.wilkins@grc.nasa.gov, lengelbert@mail.arc.nasa.gov, michael.moore@maf.nasa.gov, probles@nmo.jpl.nasa.gov, sonja.alexander@hq.nasa.gov, stephen.a.turner@maf.nasa.gov, terry.m.potterton.1@gsc.nasa.gov, tom.ambrose@dfrc.nasa.gov, wayne.kee-1@ksc.nasa.gov, Robert.Turner@hq.nasa.gov, howard.kass@hq.nasa.gov, alee@hq.nasa.gov, william.barry-1@ksc.nasa.gov, odomingu@hq.nasa.gov, Catherine.Angotti@hq.nasa.gov, mmcneill@mail.hq.nasa.gov, tspagnuo@pop200.gsc.nasa.gov, Patrick.A.Hancock.1@gsc.nasa.gov, Jim.Carter@msfc.nasa.gov, Edwin.Jones@msfc.nasa.gov, john.rodgers@hq.nasa.gov, bnotley@mail.arc.nasa.gov, gregory.l.ellis.1@gsc.nasa.gov, t.f.middleton@larc.nasa.gov, william.c.roeh1@jsc.nasa.gov, phillip.j.nessler.1@gsc.nasa.gov, pete.allen@msfc.nasa.gov, jlabrecq@hq.nasa.gov, cherbert@hq.nasa.gov, astowes@hq.nasa.gov, Ernest.M.Graham@msfc.nasa.gov, dan.thomas@hq.nasa.gov, g.m.watson@larc.nasa.gov, rdilustr@mail.hq.nasa.gov, hstewart@hq.nasa.gov, speyton@hq.nasa.gov, jlemke@hq.nasa.gov, whill@hq.nasa.gov, michael.stevens-2@ksc.nasa.gov, jllloyd@hq.nasa.gov, prichard@hq.nasa.gov, robert.t.gaffney1@jsc.nasa.gov, james.o.cheek@usago.ksc.nasa.gov, guy.camomilli-1@ksc.nasa.gov, ajohnson@mail.hq.nasa.gov

Yesterday's weather that could impact Columbia recovery. Information only. Regards, Jon
From: FEMA OPERATIONS CENTER <FEMA.OPERATIONS.CENTER@fema.gov>

To: Action Officer <ActionOfficer@fema.gov>, "ARNGOPS (E-mail)" <ARNGOPS@ngb.army.mil>, BBS Submissions <BBSSubmissions@fema.gov>, Blystadt <blystadt@usa.redcross.org>, "D'Araujo, Jack" <Jack.D'Araujo@fema.gov>, "Debbi Yamanaka (E-mail)" <dyamanaka@arrow-mountain.com>, "DOMS (E-mail)" <foxhole@doms.army.mil>, "DOT OPS - 1 (E-mail)" <tioc-01@rspa.dot.gov>, "Edward Massimo (E-mail 2)" <Edward.C.Massimo@HQ02.USACE.ARMY.MIL>.

"EPA-EOC HQ (E-mail)" <EOC.EPAHQ@epa.gov>,
"ESF-08 HHS Jevic (E-mail 2)"
<rjevec@osophs.dhhs.gov>,
FEMADESKREPS <FEMADESKREPS@fema.gov>,
"GSA Montgomery (E-mail)" <kathy.montgomery@gsa.gov>,
HSC EP&R Operations
<HSCEP&ROperations@fema.gov>,
"HUD McCarthy (E-mail)"
<bruce_e._mccarthy@hud.gov>,
"HUD Opper (E-mail)" <jan_c._opper@hud.gov>,
"James Lloyd (E-mail)" <JLloyd@hq.nasa.gov>,
"Jonathan Mullin (E-mail)"
<JMullin@hq.nasa.gov>,
"Karen Maguire (E-mail)" <karen.maguire@usda.gov>,
Mary Margaret Walker <Mary.Margaret.Walker@fema.gov>,
"Maryan Chirayath (E-mail)" <maryan.chirayath@bea.gov>,
Michael Mascaro
<michael.mascaro@bea.gov>,
"NCS (E-mail)" <NCS@NCS.GOV>,
"Nieuwejaar, Sonja" <Sonja.Nieuwejaar@fema.gov>,
"Nmci (E-mail)"
<NMCICommandCenter@eds.com>,
Northcom <icg@northcom.mil>,
"Paolin Hatch (E-mail)" <paolin.hatch@gsa.gov>,
"Parkes, Rose"
<Rose.Parkes@fema.gov>,
patti smith <patti.smith@faa.gov>,
"USACE Acosta (E-mail)" <louis.a.acosta@HQ02.USACE.ARMY.MIL>,
"USACE Hecker (E-mail)" <edward.j.hecker@usace.army.mil>,
"USACE Irwin (E-mail)" <william.e.irwin@usace.army.mil>,
"USACE Miller (E-mail)" <lizbeth.h.miller@usace.army.mil>,
USACE OPS
<ce-uoc@usace.army.mil>

Subject: FW: Status Briefing

Date: Mon, 24 Feb 2003 17:03:50 -0500

X-Mailer: Internet Mail Service (5.5.2656.59)

> -----Original Message-----
> From: R4-OPSCCELL
> Sent: Monday, February 24, 2003 5:04 PM
> To: R4-Advisory-List
> Cc: Wilson, Paul; Hollingsworth, Holly; Evans, Charleen W
> Subject: Status Briefing
>
> Attached:
>
> <<RV Status Briefing 2-24-03 12PM.doc>>

Jonathan B. Mullin
Manager Operational Safety
Emergency Preparedness Coordinator
Headquarters National Aeronautics and Space Administration
Phone (202) 358-0589
FAX (202) 358-3104
"Mission Success Starts with Safety"

 RIV Status Briefing 2-24-03 12PM.doc

X-Sender: jmullin@mail.hq.nasa.gov

X-Mailer: QUALCOMM Windows Eudora Version 4.3.2

Date: Thu, 27 Feb 2003 08:54:22 -0500

To: a.h.phillips@larc.nasa.gov, aodonogh@hq.nasa.gov, alee@hq.nasa.gov,
bdolci@arc.nasa.gov, cathy.miller@msfc.nasa.gov,
tsabikos.a.papadimitris.1@gsfc.nasa.gov, chunt@mail.arc.nasa.gov,
clyde.dease@ssc.nasa.gov, dhall@wstf.nasa.gov,
Eric.G.Fuller@jpl.nasa.gov, Ezra.R.Abrahamy@jpl.nasa.gov,
frederick.w.battle.jr@jpl.nasa.gov, h.w.beazley@larc.nasa.gov,
jack_vechil@mail.dfrc.nasa.gov, dennis.g.perrin1@jsc.nasa.gov,
luequention.wilkins@grc.nasa.gov, lengelbert@mail.arc.nasa.gov,
michael.moore@maf.nasa.gov, probles@nmo.jpl.nasa.gov,
sonja.alexander@hq.nasa.gov, stephen.a.turner@maf.nasa.gov,
terry.m.potterton.1@gsfc.nasa.gov, tom.ambrose@dfrc.nasa.gov,
wayne.kee-1@ksc.nasa.gov, Robert.Turner@hq.nasa.gov,
howard.kass@hq.nasa.gov, alee@hq.nasa.gov,
william.barry-1@ksc.nasa.gov, odomingu@hq.nasa.gov,
Catherine.Angotti@hq.nasa.gov, mmcneill@mail.hq.nasa.gov,
tspagnuo@pop200.gsfc.nasa.gov, Patrick.A.Hancock.1@gsfc.nasa.gov,
Jim.Carter@msfc.nasa.gov, Edwin.Jones@msfc.nasa.gov,
john.rodgers@hq.nasa.gov, bnotley@mail.arc.nasa.gov,
gregory.l.ellis.1@gsfc.nasa.gov, t.f.middleton@larc.nasa.gov,
william.c.roeh1@jsc.nasa.gov, phillip.j.nessler.1@gsfc.nasa.gov,
pete.allen@msfc.nasa.gov, jlabrecq@hq.nasa.gov, cherbert@hq.nasa.gov,
astowes@hq.nasa.gov, Ernest.M.Graham@msfc.nasa.gov,
dan.thomas@hq.nasa.gov, g.m.watson@larc.nasa.gov,
rdilustr@mail.hq.nasa.gov, hstewart@hq.nasa.gov, speyton@hq.nasa.gov,
jlemke@hq.nasa.gov, whill@hq.nasa.gov, michael.stevens-2@ksc.nasa.gov,
jilloyd@hq.nasa.gov, prichard@hq.nasa.gov,
robert.t.gaffney1@jsc.nasa.gov, james.o.cheek@usago.ksc.nasa.gov,
guy.camomilli-1@ksc.nasa.gov, ajohnson@mail.hq.nasa.gov

From: "Jonathan B. Mullin" <jmullin@hq.nasa.gov>

Subject: Fwd: FW: FEMA Incident Update Report, FEMA Region VI, Winter
Storm 02- 23-03

Weather factors that may affect Columbia activities. Regards, Jon

From: FEMA OPERATIONS CENTER <FEMA.OPERATIONS.CENTER@fema.gov>

To: Action Officer <ActionOfficer@fema.gov>,
"AOC (E-mail)"

<agstenos@hqda-aoc.army.pentagon.mil>,
ARNGOPS <ARNGOPS@ngb.army.mil>,
"BBS Submissions (E-mail) (E-mail)" <BBSSubmissions@fema.gov>,
"Bothell MOC (E-mail) (E-mail)" <Bothell.MOC@fema.gov>,
"Brian Montgomery (E-mail)" <brian.montgomery@fema.gov>,
"Cameron, Bruce"

<Bruce.Cameron@fema.gov>,
Charles Stewart <Charles.Stewart@navy.mil>,
"D'Araujo, Jack" <Jack.D'Araujo@fema.gov>,
David Fleischman

<David_Fleischman@hud.gov>, "Debbi Yamanaka (E-mail)" <dyamanaka@arrow-mountain.com>, "Denton MOC (E-mail)" <Denton.MOC@fema.gov>, "Denver MOC (E-mail)" <Denver.MOC@fema.gov>, DOE <rsp.div@hq.doe.gov>, "DOEHQEOC (E-mail)" <DOEHQEOC@OEM.DOE.GOV>, "DOI OPS CENTER (E-mail)" <doi_watch_center@ios.doi.gov>, "Earman, Margie" <Margie.Earman@fema.gov>, "Edward Massimo (E-mail 2)" <Edward.C.Massimo@HQ02.USACE.ARMY.MIL>, EMAC <emac@adem.state.ar.us>, "EPA-EOC HQ (E-mail)" <EOC.EPAHQ@epa.gov>, EST-DIR <EST-DIR@fema.gov>, "FCC Bonnie Gay (E-mail)" <bgay@fcc.gov>, "FEMA HSCenter (E-mail)" <FEMA.HSCenter@DHS.GOV>, FEMADESKREPS <FEMADESKREPS@fema.gov>, "GRACE. SHEFFEY (E-mail)" <GRACE.SHEFFEY@FNS.USDA.GOV>, "GSA Montgomery (E-mail)" <kathy.montgomery@gsa.gov>, "gsa. nsep@gsa. gov (E-mail)" <gsa.nsep@gsa.gov>, "Hess, Charles" <Charles.Hess@fema.gov>, "Homeland Security (E-mail)" <ohscc@who.eop.gov>, "HUD McCarthy (E-mail)" <bruce_e._mccarthy@hud.gov>, "HUD Opper (E-mail)" <jan_c._opper@hud.gov>, "James Lloyd (E-mail)" <JLloyd@hq.nasa.gov>, "Jerry Ostendorf (E-mail)" <jerry.ostendorf@emd.state.ia.us>, "Jonathan Mullin (E-mail)" <JMullin@hq.nasa.gov>, "Karen Maguire (E-mail)" <karen.maguire@usda.gov>, "Lowder, Michael" <Michael.Lowder@fema.gov>, "Maynard MOC (E-mail)" <Maynard.MOC@fema.gov>, "Naval District, Washington - Security and LE Dir." <Stewart.Charles@ndw.navy.mil>, "NCS (E-mail)" <NCS@NCS.GOV>, "NIGHT1 (E-mail)" <NIGHT1@USA.REDCROSS.ORG>, "Nmci (E-mail)" <NMCICommandCenter@eds.com>, "Nora Lewis (E-mail)" <nlewis@USAID.GOV>, Northcom <icg@northcom.mil>, "NORTHCOM LNO Todd Chamberlain (E-mail)" <todd.chamberlain@js.pentagon.mil>, "NORTHCOM Robert Price (E-mail)" <robert.price@northcom.mil>, "Paolin Hatch (E-mail)"

<paolin.hatch@gsa.gov>,
"ROSTOSKYC (E-mail)"
<ROSTOSKYC@USA.REDCROSS.ORG>,
"Russell, Barbara"
<Barbara.Russell@fema.gov>,
"Thomasville MOC (E-mail)"
<Thomasville.MOC@fema.gov>,
"Zensinger, Larry"
<Larry.Zensinger@fema.gov>,
"DOD/DOMS Lacrosse (E-mail)"
<thomas.lacrosse@doms.army.mil>,
"DOMS (E-mail)" <foxhole@doms.army.mil>,
DOMS Sullivan <ricki.sullivan@doms.army.mil>,
"Porter, Larry"
<Larry.Porter@fema.gov>,
"Riddle, Margaret" <Margaret.Riddle@fema.gov>,
"DOT Benini (E-mail)" <janet.benini@rspa.dot.gov>,
"DOT Carney (E-mail)"
<brian.carney@rspa.dot.gov>,
"DOT Medigovich (E-mail)"
<bill.medigovich@rspa.dot.gov>,
"DOT OPS - 1 (E-mail)"
<tioc-01@rspa.dot.gov>,
"DOT OPS 2 (E-mail)" <tioc-02@rspa.dot.gov>,
"HOWARD. EDWARDS (E-mail)" <HOWARD.EDWARDS@rspa.dot.gov>,
"USACE Acosta (E-mail)" <louis.a.acosta@HQ02.USACE.ARMY.MIL>,
"USACE Hecker (E-mail)" <edward.j.hecker@usace.army.mil>,
"USACE Irwin (E-mail)" <william.e.irwin@usace.army.mil>,
"USACE Miller (E-mail)" <lizabeth.h.miller@usace.army.mil>,
USACE OPS
<ce-uoc@usace.army.mil>

Subject: FW: FEMA Incident Update Report, FEMA Region VI, Winter Storm 02-23-03

Date: Wed, 26 Feb 2003 16:53:08 -0500

X-Mailer: Internet Mail Service (5.5.2656.59)

> ---Original Message---
> From: R06-ROC-DIR
> Sent: Wednesday, February 26, 2003 4:44 PM
> To: FEMA OPERATIONS CENTER; MOC, Denton; 'FEMA.HSCenter@DHS.gov';
> 'icg@northcom.mil'
> Subject: FEMA Incident Update Report, FEMA Region VI, Winter Storm
> 02-23-03
>
> <<RV1-Winter Storm-02-23-03 Update 1A.doc>>
>

Jonathan B. Mullin

Jonathan B. Mullin, 08:54 AM 2/27/2003 -0500, Fwd: FW: FEMA Incident Update Report, FEMA Reg

Manager Operational Safety
Emergency Preparedness Coordinator
Headquarters National Aeronautics and Space Administration
Phone (202) 358-0589
FAX (202) 358-3104
"Mission Success Starts with Safety"



RVI-Winter Storm-02-23-03 Update 1A.doc

Incident Name: RVI-Winter Storm-02-23-03
Category: Incident
Type: Winter Storm
Status: Open

Occurred Date: 02/23/2003 00:00:00
Reported Date: 02/25/2003 16:52:54
Reported By: MDUGAN
Contact: Ron Castleman, RD, 940
898-5104; Gary Jones,
DRD, 898-5123; Brenda
Black, RR Director, 898-
5146

States Impacted: AR, OK, TX

Description:

Beginning on February 23, 2003, a strong winter storm moved south through Oklahoma, Arkansas and Texas bringing a mix of rain, sleet, freezing rain, and snow and producing wind chill effects into the teens and twenties. Total ice accumulations in excess of a quarter of an inch are being experienced making area roadway travel extremely hazardous. The system has caused significant air traffic delays at area airports. Isolated power outages have been reported throughout the three state area but all have been quickly addressed. Several ARC shelters were opened in Oklahoma. Contact has been made with all three states and none have reported any significant issues. Precipitation should end Tuesday as the storm system moves east out of the region. Situation updates from Texas and Oklahoma are expected by noon CST. The region will continue to monitor the situation.

From: MDUGAN

Date: 02/23/2003 21:09:11

Subject: RVI-WINTER STORM-02-23-03 UPDATE 1

Message:

There has been no significant change to the situation in Texas, Oklahoma and Arkansas. Ice on roadways continues to make ground travel extremely hazardous especially along the I-35 corridor from north of Perry, Oklahoma to Austin, Texas. Weather conditions are expected to improve this afternoon with refreezing occurring overnight north of I-20. Sustained temperatures above the freezing point are not expected until the late morning hours on Thursday in the Dallas/Fort Worth/Denton, Texas area after which road conditions should gradually improve. There will be a 30-60 percent chance of additional snow accumulation today in Oklahoma with a possibility of rain and snow mix on Thursday and Friday. Recorded snowfall amounts exceed twelve inches in seven Oklahoma counties.

Rescuing and sheltering stranded motorists was the major problem being addressed by local officials during the overnight hours. Overall, the power situation remains good in all three states with the exception of a report of 8000 customers in South/Central Arkansas currently without power. Power is expected to be restored in that area by Friday.

Two fatalities and two injuries have been attributed to this weather system in Texas. One fatality was reported in Oklahoma.

The FEMA Region VI office implemented its severe weather plan on February 25 and 26 with only essential personnel being required to report for work. A decision on tomorrow's Regional Office work hours will be made at 7PM tonight based on input from the National Weather Service and the Texas Department of Transportation.

There continues to be no request for federal assistance. FEMA Region VI will continue to monitor the situation.

"Edward Massimo (E-mail 2)" <Edward.C.Massimo@HQ02.USACE.ARMY.MIL>,
"EPA-EOC HQ (E-mail)" <EOC.EPAHQ@epa.gov>,
"ESF-08 HHS Jevenc (E-mail 2)"
<rjevenc@osophs.dhhs.gov>,
"GSA Montgomery (E-mail)"
<kathy.montgomery@gsa.gov>,
"HUD McCarthy (E-mail)"
<bruce_e._mccarthy@hud.gov>,
"HUD Opper (E-mail)" <jan_c._opper@hud.gov>,
"James Lloyd (E-mail)" <JLloyd@hq.nasa.gov>,
"Jonathan Mullin (E-mail)"
<JMullin@hq.nasa.gov>,
"Karen Maguire (E-mail)" <karen.maguire@usda.gov>,
Mary Margaret Walker <Mary.Margaret.Walker@fema.gov>,
"Maryan Chirayath (E-mail)" <maryan.chirayath@bea.gov>,
Michael Mascaro
<michael.mascaro@bea.gov>,
"NCS (E-mail)" <NCS@NCS.GOV>,
"Nieuwejaar, Sonja" <Sonja.Nieuwejaar@fema.gov>,
"Nmci (E-mail)"
<NMCICommandCenter@eds.com>,
"Paolin Hatch (E-mail)"
<paolin.hatch@gsa.gov>,
"Parkes, Rose" <Rose.Parkes@fema.gov>,
"USACE Acosta (E-mail)" <louis.a.acosta@HQ02.USACE.ARMY.MIL>,
"USACE Aguilera (E-mail)" <karen.durham-aguilera@usace.army.mil>,
"USACE Gilmore (E-mail)" <george.l.gilmore@usace.army.mil>,
"USACE Hecker (E-mail)" <edward.j.hecker@usace.army.mil>,
"USACE Irwin (E-mail)" <william.e.irwin@usace.army.mil>,
"USACE Miller (E-mail)" <lizabeth.h.miller@usace.army.mil>,
USACE OPS
<ce-uoc@usace.army.mil>

Subject: FW: [Nipcdaily-list] NIPC Daily Open Source Report 11 Feb 2003

Date: Tue, 11 Feb 2003 07:23:43 -0500

X-Mailer: Internet Mail Service (5.5.2656.59)

-----Original Message-----

From: nipcdaily-list@mail.nipc.osis.gov

[mailto:nipcdaily-list@mail.nipc.osis.gov]

Sent: Tuesday, February 11, 2003 7:18 AM

To: nipcdaily-list@mail.nipc.osis.gov

Subject: [Nipcdaily-list] NIPC Daily Open Source Report 11 Feb 2003

The NIPC Daily Open Source Report is attached. It is a summary of open-source published information concerning significant critical infrastructure issues. Readers wishing to comment on the contents or

suggest additional topics and sources should contact NIPC Daily Report Team at nipcdailyadmin@mail.nipc.osis.gov or call 202-324-1131 or 202-324-1129.

Requests for adding or dropping subscription to the NIPC Daily Open Source Report should be sent to nipcdailyadmin@mail.nipc.osis.gov.

Additionally, many readers should note that the NIPC Daily Open Source Report is currently being published in PDF format. The reader software is free and can be downloaded from <http://www.adobe.com/products/acrobat/readstep2.html>.

Should you have problems or concerns related to the format of the Daily Report, please send an email to nipcdailyadmin@mail.nipc.osis.gov. The daily is now being distributed via a new distribution service. While we have spent significant time preparing for the transition, there will undoubtedly be some transition issues. Please send problems, comments, etc to nipcdailyadmin@mail.nipc.osis.gov.

The NIPC Daily Report Team

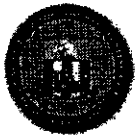
Jonathan B. Mullin
Manager Operational Safety
Emergency Preparedness Coordinator
Headquarters National Aeronautics and Space Administration
Phone (202) 358-0589
FAX (202) 358-3104
"Mission Success Starts with Safety"



[NIPC Daily 2003-02-11.pdf](#)



[ATT1220321.txt](#)



National Infrastructure Protection Center NIPC Daily Open Source Report for 11 February 2003

Current Nationwide
Threat Level is



For info click here
www.whitehouse.gov/homeland

Daily Overview

- CNN reports that according to the Lundberg Survey released on Sunday, the average price of a gallon of gasoline nationwide has gone up more than 11 cents during the past two weeks, mainly caused by Venezuela's general strike and international preparations for a possible war in Iraq. (See item 4)
- Reuters reports the Russian Defense Minister Sergei Ivanov said on Saturday that use of the deadly toxin ricin could be traced back to Chechen rebels, and makeshift laboratories had been found in Georgia's Pankisi Gorge. (See item 10)
- The Associated Press reports the U.S. Coast Guard is stepping up its presence on the water and in the air at the nation's ports now that the country is at its second-highest terror alert status, and vessel movements are being monitored through both local and national surveillance tracking systems. (See item 18)
- The Medill News Service reports Dartmouth College's Institute for Security Technology Studies has charted how political cyberattacks often precede physical attacks noting that cyberattacks after U.S.-led military action are "extremely likely" and could possibly be catastrophic. (See item 32)
- Note from the Editor: As of 3 February, the NIPC Daily Open Source Report is being distributed through a new list service. While significant effort has been done to ensure smooth transition, problems are bound to occur. Please notify nipcdailyadmin@mail.nipc.osis.gov with any comments, concerns, questions, or problems.
- Note from the Editor: Both the PDF and Word versions of the daily are posted to the NIPC Web Site at <http://www.nipc.gov/dailyreports/dailyindex.htm>

NIPC Update Fast Jump

Production Industries: Energy; Chemical; Defense Industrial Base

Service Industries: Banking and Finance; Transportation; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information and Telecommunications; Internet Alert Dashboard

Other: General; NIPC Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: High, Cyber: High

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - <http://esisac.com>]

- 1. February 10, Reuters — U.S. oil industry raises security on attack warning. The U.S. oil industry has raised security at the nation's refineries, pipelines, ports and production facilities following a White House announcement that threat of attacks on American targets had increased, the American Petroleum Institute said Friday. "We have shared information from the National Infrastructure Protection Center regarding the threat and our members have increased measures to secure their facilities," said Kendra Martin, director of security at the API, the nation's largest oil industry group. In response to the heightened threat, the U.S. Coast Guard said Friday it will increase patrols in New York Harbor and other waterways, while other groups representing the oil and chemical industry said they are already guarded. The East Harris County Manufacturers Association, which has 125 members made up of chemical plant and petroleum refineries along the refinery-row bordering the Houston Ship Channel, said it is prepared for the heightened alert.**

Source: http://www.forbes.com/home_europe/newswire/2003/02/07/rtr874_146.html
- 2. February 10, Platts Global Energy News — U.S. becoming overly dependent on gas, senator says. U.S. Senate Energy and Natural Resources Committee Chairman Pete Domenici Monday expressed concern about the U.S. becoming overly reliant on gas. In a Washington speech to the American Public Power Association, Domenici said that he has been told that gas is "here in abundance" and the U.S. will never run out of domestic supply. "I want to believe 'em," he said. But Domenici said he fears that the U.S. "has grown dependent on gas," pointing to the fact that most of the power plants constructed over the past decade have been gas-fired. At the same time, Domenici said he wants to take steps to improve access to coal-bed methane located on public land. Domenici indicated that steps should be taken to improve the process for obtaining a permit to develop gas on land currently available for development.**

Source: <http://www.platts.com/stories/gas1.html>
- 3. February 10, Reuters — The United States expressed grave concern on Monday that Iran, the third member of its "axis of evil", was trying to develop nuclear weapons after reporting ambitious atomic energy plans. The head of Iran's atomic energy organisation, Gholamreza Aqazadeh, said his country was poised to begin processing uranium for its atomic energy programme. A signatory to nuclear non-proliferation pacts, Iran insists its programme is purely peaceful and has invited U.N. inspectors to verify its nuclear facilities later this month. "Iran's ambitious and costly pursuit of a complete nuclear fuel cycle only makes sense if it's in support of a nuclear weapons programme," he told a daily briefing. Iran intended to control the whole fuel cycle, from mining and enriching uranium to managing spent fuel. Western diplomats linked the timing of Iran's announcement to the planned visit of an inspection team this month headed by ElBaradei.**

Source: http://www.energycentral.com/sections/newsroom/nr_article.cf m?id=3634591

4. *February 09, CNN* — **Gas prices skyrocket around United States.** Concerns over Iraq, Venezuela raise average cost 11 cents Americans are digging deeper at their gas pumps. **According to a survey released Sunday, the average price of a gallon of gasoline nationwide has gone up more than 11 cents during the past two weeks.** Americans paid an average of \$1.60 per gallon of self-serve regular, the Lundberg Survey said. Publisher Trilby Lundberg said that is the highest price at the pump since June 2001. **The price increase is in keeping with the rise in crude oil prices, which have exceeded \$35 per barrel — up more than \$8 per barrel during the past two months, Lundberg said. The "two big reasons," she said, are an oil shortage caused by Venezuela's general strike and international preparations for a possible war in Iraq.** According to the Department of Energy, Venezuela was the fourth-largest exporter of crude oil to the United States in November, before the strike began. Iraq, with the world's second-largest proven oil reserves, is the ninth-largest exporter to the United States. Concerns about the possible loss of Iraq's supply have affected the price of gasoline because on futures markets, "oil prices rise on fears and perceptions, not just supply and demand," Lundberg said.

Source: <http://www.cnn.com/2003/US/02/09/gas.prices/index.html>

5. *February 09, Concord Monitor (New Hampshire)* — **Seabrook wants \$1 million state subsidy. In a proposal closely watched by national nuclear lobbyists, Seabrook Station (in New Hampshire) is asking state environmental regulators for a \$1 million subsidy designed for clean power producers. New Hampshire would become the first state in the nation to extend the subsidy to a nuclear plant – setting a precedent that supporters and critics alike believe other states would likely follow.** The state Department of Environmental Services currently gives out the subsidy – which can be sold to other plants – to encourage oil-fired, coal-fired, gas-fired and hydroelectric power plants to voluntarily reduce their emissions of smog-causing nitrogen oxide. Under a proposal now being advanced by the department, the credit would be extended to Seabrook for not emitting any nitrogen oxide whatsoever. Seabrook, championed by former Republican governors Meldrim Thomson and John Sununu, always has stirred strong feelings in New Hampshire residents. **In 1977, more than 1,400 people were arrested and detained for nearly two weeks after a protest against the plant's construction. But in 1989, lawmakers rallied behind Public Service Company of New Hampshire, the plant's owner at the time, and allowed the utility to raise customer electric rates to cover Seabrook's ballooning construction cost overruns.** The plant was recently sold to Florida Light and Power, which has formally made the request for the pollution credits. The industry's executives and lobbyists – plagued for decades by public-image disasters including meltdowns at Chernobyl and Three Mile Island that released massive amounts of radiation into surrounding communities – have lately embarked on an effort to persuade the public that nuclear power is, in fact, a clean, green source of electricity. The Nuclear Energy Institute, the industry's leading lobbying group, calls nuclear "the clean air energy."

Source: http://www.cmonitor.com/stories/news/local2003/0209_nukesubs_idy_2003.shtml

6. *February 09, Efe* — **Venezuela grants gas exploration rights to foreign firms. The Venezuelan government granted gas-exploration rights to Norway's Statoil and U.S.-based Chevron-Texaco for the Plataforma Deltana region, Venezuela's largest gas field.** Energy and Mines Minister Rafael Ramirez said Saturday that Chevron-Texaco paid \$19 million for the rights to explore Plataforma Deltana's block 2, while Statoil offered \$32 million

for the license to explore block 4.

Source: http://www.energycentral.com/sections/gasnews/gn_article.cfm?id=3634653

7. *February 07, Platts Global Energy News* — **NRC advises licensees to increase security. The Nuclear Regulatory Commission (NRC) has advised licensees to adopt the additional security measures that correspond to the Feb. 7 increase of the Homeland Security Department's threat advisory level from "yellow" to "orange," agency spokesperson Beth Hayden said.** Hayden declined to identify any specific security measures to be taken under the latest threat advisory. According to an Aug. 12, 2002 regulatory issue summary, **protective measures that generally correspond to the orange threat condition assume that a plant operator's security organization is at its highest sustainable level and that the licensee will request augmentation by local and state, and possibly federal, resources to provide additional defensive capabilities to the extent such resources can be made available.**

Source: <http://www.platts.com/stories/nuclear1.html>

[\[Return to top\]](#)

Chemical Sector

8. *February 10, New York Times* — **U.N. conference backs efforts to curb mercury pollution.** Delegates attending a United Nations environmental conference here last week endorsed a global crackdown on pollution caused by mercury, although the United States blocked efforts for binding restrictions on its use. **Mercury, a highly toxic heavy metal, is particularly dangerous for infants and children, and it can be passed from pregnant women to their fetuses. Human exposure to mercury comes from a variety of sources — consumption of fish, occupational and household uses, dental fillings and some vaccines. The United Nations Environment Program will begin assisting countries, particularly those in the developing world, in devising methods for cutting emissions of mercury from sources like coal-fired power stations and incinerators. Further action, possibly including a binding protocol, was put off until 2005.** The decision followed the release of a report outlining a significant global threat to humans and wildlife from mercury, a naturally occurring metal. Mercury exposure can cause development problems and can affect the brain, kidneys and liver. The conference drew more than 1,000 delegates from 130 nations. The delegates agreed that "there is sufficient evidence of significant global adverse impacts from mercury and its compounds to warrant further international action to reduce the risks to human health and the environment." **The United Nations report found that mercury travels throughout the earth at a far greater rate than was previously known, circulating between the air, water and soil as well as in living things. Even regions without significant mercury releases of their own, such as the Arctic, were found to be adversely affected by the global spread of mercury.** Mercury has many industrial applications, although safer alternatives exist. It is used in small-scale mining of gold and silver as well as in thermometers, fluorescent lamps and some paints. The substance is also contained in many skin-lightening creams as well as in some traditional medicines.

Source: <http://www.nytimes.com/2003/02/10/international/africa/10NAIR.html>

9. *February 08, Associated Press* — **Common chemicals may be used by terrorists. A variety of chemicals commonly used in industry also could also be used to mount a terror attack.**

Much of the nation's attention has focused on the threat of biological attacks that would use anthrax, smallpox or other pathogens. But just last month, the deadly poison ricin was found in a north London apartment. **Used as weapons, many chemicals could maim, kill, and pose risks to the public, although a review of the chemical terror threat concluded that specialized knowledge would be needed to acquire and deliver most of them effectively.** "In most cases terrorists would have to overcome significant technical and operational challenges," the General Accounting Office (GAO), Congress' investigative arm, said in 1999 testimony. **But not always, the GAO said: "Some chemical agents are commercially available and require little sophistication or expertise to obtain or use."** For instance, toxic industrial chemicals such as chlorine, phosgene, and hydrogen cyanide are readily available. These are among the earliest chemical weapons and were used by troops in World War I. Today, they are commonly used in commercial manufacturing and "could be easily adapted as terrorist weapons," the GAO said. Cyanide, for instance, is commonly used in electroplating, where metals are attached to each other, and jewelry manufacturing. It's not alone on the threat list. **Commercial pesticides such as organophosphates, commonly available in hardware stores, are far less deadly than nerve agents like sarin or soman, but they produce similar effects in the body by poisoning the nervous system.** Chemicals could be delivered relatively effectively through indoor ventilation systems or in food or water. **The most deadly agents in the chemical arsenal are nerve agents, although they are more difficult to obtain.** A small amount of sarin or soman can penetrate the lungs or the skin and invade the nervous system. Sarin has been used once before: **In 1995, the Japanese cult Aum Shinrikyo released it into the Tokyo subway system, killing 12 and sickening thousands.** The most toxic of chemical weapons is VX, a sticky, colorless liquid that evaporates slowly into a colorless, odorless gas. **A dose of 10 milligrams on the skin is enough to kill.**

Source: <http://www.thedesertsun.com/news/stories/national/1044674666.shtml>

10. *February 08, Reuters* — **Russia says ricin can be traced to Chechen rebels.** Russian Defense Minister Sergei Ivanov said on Saturday that use of the deadly toxin ricin could be traced back to Chechen rebels, and makeshift laboratories had been found in Georgia's Pankisi Gorge. Speaking at a security conference in Munich, Ivanov said "Chechen-brand terrorism" was an intrinsic part of alleged terrorist activities which have surfaced recently in various countries, including France and Britain. "As for the training and instruction base for the international chemical terrorists, it is a well-known destination — the Pankisi Gorge in Georgia," he said. **"Down there, makeshift ricin laboratories have been found. The recently captured chemical terrorists apprehended in France and the United Kingdom had been undergoing training there."**

Source: http://story.news.yahoo.com/news?tmpl=story&s_nm/russia_chechnya_dc_1

[[Return to top](#)]

Defense Industrial Base Sector

11. *February 10, Washington Post* — **U.S. military in Europe may change.** The United States is contemplating radically changing the nature of its military presence in Europe, moving from a "garrison" system of big, heavily staffed Cold War-era bases to a more expeditionary posture in which troops would be deployed to the continent on a rotational basis, said members of the U.S. delegation flying home yesterday from an annual conference on security issues in Munich.

If implemented, the change would be one of the biggest in the history of U.S. military bases in Europe, which dates to the end of World War II. Even discussing the shift sends the signal in Europe that the United States is ready to match changes in the alliance's political structure with changes in its military structure. Disclosure of the move also might be interpreted in Europe, especially in Germany, as a sign that the United States is exploring alternatives to its heavy reliance on Germany as the host of its core military operations in Europe. Several members of the delegation spoke enthusiastically at the briefing they were given by Marine Gen. James Jones, the new U.S. commander in Europe, on his preliminary thoughts about possible ways to overhaul the U.S. military presence in Germany and elsewhere in Europe. They said they expect a permanent U.S. military presence eventually to be cut from the current level of about 100,000 personnel, most of them Army. Rather, they said Jones and other top Defense Department officials are contemplating something more akin to the U.S. presence in Kuwait, where tanks, trucks and other military gear are stored, with troops flying in to exercise or deploy with it. **Sen. John McCain (R-Ariz.), one of those briefed by Jones, said that the commander "envisions a transition to bases with prepositioned equipment and skeleton crews." That makeover would reduce the U.S. military presence in Europe by closing facilities such as Defense Department schools and military commissaries but ultimately might make U.S. bases in Germany more important to U.S. strategy. In a few years, some of the Pentagon officials said, the U.S. bases in Germany, Britain and Italy could be what the military calls "power projection" platforms from which forces could move quickly to hot spots in the Middle East, Africa or Asia. Some U.S. troops are moving from bases in Germany to the Persian Gulf region, but they are not configured for rapid deployment. Rep. Jane Harman (D-Calif.), who also attended Jones's briefing, said, "He was talking about a different configuration that is more nimble and flexible."**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A49179-2003Feb9.html>

12. *February 07, Aerospace Daily* — **Bandwidth needs may not make DoD turn to private sector, analysts say.** Despite the U.S. military's growing need for bandwidth, the likelihood that it will turn increasingly to the commercial satellite industry to fulfill that need remains remote, according to some industry analysts. **The military always will depend on the commercial sector for some of its communications needs, such as casual communication, analysts say, but budget issues and the military's unique needs may make longer-term relationships difficult.** "We will never have enough military satellite capability and bandwidth-protected satellites to satisfy what the wartime commander needs," Lt. Gen. Joseph Kellogg Jr. said this week at the 2003 Defense Excellence conference, sponsored by the American Institute of Aeronautics and Astronautics. Kellogg, director of Command, Control, Communications and Computer Systems (C4) for the Joint Chiefs of Staff, said he is confident about having sufficient UHF capability for the military. **"But when we come to the VHF area and the commercial activities ... we're always going to rely on [commercial providers]," Kellogg said. "We don't have the money to put into all of those [communications networks]." Those financial straits also will prevent the military from buying more existing bandwidth, Kellogg added. Eventually, laser communications will give the military "tremendous capacity," he said, referring to Defense Department plans for a network of satellites connected by lasers.**

Source: <http://ebird.dtic.mil/Feb2003/s20030207152594.html>

[Return to top]

Banking and Finance Sector

13. *February 06, Reuters* — **U.S. aims to stiffen identity theft shield—official.** The U.S. Treasury Department plans to step up efforts to prevent identity theft, which can result in one person running up ruinous bills in another person's name, a senior official said on Thursday. **Treasury is putting together a package of legislative proposals to deter identity thieves, Assistant Treasury Secretary for Financial Institutions Wayne Abernathy told reporters. An important goal is to quickly restore the credit rating of people who have been unknowingly saddled with massive debt by someone else who has used their Social Security number or other personal information, Abernathy said after speaking to the National Association of Affordable Housing Lenders.** Banks need to be allowed to continue sharing information about their customers with other financial institutions, he said. This helps law enforcement officials to quickly contact a victim's creditors and discover all of the ways that person's financial privacy has been violated, Abernathy said. **To this end, he called for Congress to renew the Fair Credit Reporting Act, due to expire this year, or state laws curtailing information-sharing by financial institutions would take precedence. "The first thing you need to do in that regard is we need to make the FCRA, a uniform national standard, permanent," he said.**

Source: http://story.news.yahoo.com/news?tmpl=story24206/ts_nm/crime_identity_dc_2

[Return to top]

Transportation Sector

14. *February 11, Independent.co.uk News* — **Troops deployed at Heathrow against terror threat. More than 400 soldiers were drafted in to provide extra security at Heathrow Airport and a number of other unspecified sites across London today to combat a new terrorist threat.** Troops began to take up their new positions at one of the world's busiest international airports at 6am and will be deployed throughout the rest of the day as part of a "contingency plan" authorised by the Government and the Metropolitan Police. The "precautionary measure" is linked to a new **fear that al-Qa'ida could use the end of the Muslim festival of Eid, which runs from tomorrow until Saturday, as a trigger for attacks.** "To avoid prejudicing ongoing operations, we do not intend to give any further details of security arrangements, other than to say that this action is in line with the policy of taking whatever action we believe necessary to protect the public." Strengthened security would be most visible at Heathrow but other sites would be on higher alert and troops would remain "for as long as the Metropolitan Police requires our assistance", said a spokesman for the Ministry of Defence. The intended arrangement includes the use of military personnel in support of the Met Police." Mick Temple, managing director at Heathrow, said: "Safety and security for passengers and staff is our top priority. Mike Yardley, an expert on terrorism, said: **"This is a message to anyone with ill intent that we are prepared to beef up security at these installations and that they are likely to receive a hot reception.**" It is sending a message to terrorists and to people who use airports that we are taking precautions.

Source: http://news.independent.co.uk/uk/this_britain/story.jsp?story=377426

15. *February 10, Government Computer News* — **Change in DOT will result in more funds for FAA systems, CIO says. The Transportation Department plans to spend most of its fiscal 2004 IT funding on the Federal Aviation Administration's air traffic systems modernization and on DOT telecommunications programs.** The budget proposal that President Bush sent to Congress this month earmarked \$2.6 billion for IT at Transportation. The department would allocate \$660 million for FAA's systems and \$400 million for telecom projects, said Eugene "Kim" Taylor, the department's acting CIO. Now that the Transportation Security Administration and the Coast Guard are moving to the new Homeland Security Department, more funds are available for FAA systems, he said. **Transportation plans to allocate more funds for FAA systems such the Standard Terminal Automation Replacement System and the Integrated Terminal Weather System, he said. In its role as overseer of Transportation programs, the CIO office plans to spend \$25 million on capital planning, enterprise architecture and cybersecurity efforts.** "Cybersecurity is clearly high on our list to make sure our program is solid and protected across the department," he said. Source: http://www.gcn.com/vol1_no1/daily-updates/21130-1.html

16. *February 10, MaineToday.com* — **UMA professor learns airport security tactics: Israeli conference gives insight for Maine program.** The security tactics used by police officers assigned to the state of Maine's commercial airports will undergo a major overhaul this year — but the man in charge of implementing the training program said he hopes no one notices the change. Richard Mears, a criminal justice professor at the University of Maine at Augusta, said he hopes that, by the end of this year, officers providing airport security will be able to identify and question possible security threats before they reach bag-screening areas — and without disturbing other travelers. "What I hope to do is get us out ahead of the curve, instead of reacting to incidents after they happen," Mears said. Currently, police departments schedule officers to work an airport shift based primarily on who is available — not on whether they have received any training geared toward identifying possible threats to airline travelers. Mears said he hopes to change that. "I travel a lot in the United States, and I've seen a wide disparity in what the officers are doing," he said. "Trained officers (are) more aware of what to look for, their attention is focused in different areas." **His program, which will be developed over the next two months and implemented at police departments throughout the state later this year, will be based on tactics already used by Israeli security officials at El Al Airlines. Although Mears would not divulge the exact nature of the new program for security reasons, he said training will focus on identifying suspicious travelers by their demeanor rather than what they look like.**

Source: http://www.centralmaine.com/news/stories/030210mears_kj.shtm |

17. *February 09, Times Herald (Michigan)* — **Terror alert slows border crossings.** The threat of terrorism on Saturday hung over area border crossings — enough for travelers to notice. "They've been holding us up," said Robert Sanford, operations manager at City Cab Inc. in Port Huron, MI. Sanford said **taxi drivers crossing the Blue Water Bridge in Port Huron experienced waits of up to 45 minutes at various times Friday and Saturday due to increased border-security measures.** The extra precautions are due to the federal government's orange alert, a warning the United States faces a "high-risk" of terrorism attacks. **U.S. Customs officials, as well as U.S. Border Patrol agents, this weekend increased the number of vehicle inspections at the Blue Water Bridge and the ferry crossing from Sombra, Ontario, to Marine City, as well as at Detroit's Ambassador Bridge and the**

Detroit-Windsor Tunnel. While frequent travelers in Detroit couldn't use NEXUS express lane cards to bypass questioning on the Ambassador Bridge, NEXUS lanes on the Blue Water Bridge functioned normally.

Source: <http://www.thetimesherald.com/news/stories/20030209/localnews/950281.html>

[[Return to top](#)]

Postal and Shipping Sector

18. *February 07, Associated Press* — **Coast Guard increases port security in light of terror alert.** The U.S. Coast Guard is stepping up its presence on the water and in the air at the nation's ports now that the country is at its second-highest terror alert status. **"We are increasing our homeland security patrols using our boats, ships and aircraft," Lt. Cmdr. Brendan McPherson, spokesman for the Coast Guard's Portsmouth-based Atlantic Area Command, said Friday.** "Cutters and aircraft in maintenance and standby status are being put on alert and made ready to get underway if needed or directed to do so." McPherson said boaters and mariners can expect to see a greater Coast Guard presence. "They should be prepared to be interrogated or questioned about their activity, particularly if they're operating or loitering in an area that might be of concern," such as naval facilities, McPherson said. "We would advise, if they don't need to be there, they should stay clear of those areas." **Local captains of the ports are assessing security within their ports and adding additional security zones where needed, McPherson said, and vessel movements are being monitored through both local and national surveillance tracking systems. The Coast Guard also is asking anyone who uses ports and waterways to be on alert and report any unusual or suspicious activity, McPherson said.**

Source: <http://www.dailypress.com/news/local/virginia/dp-va--terror-alert-ports0207feb07.0.1995080.story?coll=dp-headlines-virginia>

19. *February 07, U.S. Customs Service* — **U.S. Customs Service statement on change to alert level orange.** Consistent with the nationwide increase to Alert Level Orange [High], the U.S. Customs Service is increasing border security activities at all the nation's ports of entry. **Under Alert Level Orange, U.S. Customs implements additional security precautions, including increased vehicle, passenger, cargo, and mail examinations.** Businesses and travelers can obtain information about border wait times at the U.S. Customs Service web site: www.customs.gov.

Source: http://www.customs.gov/xp/cgov/newsroom/press_releases/02072_003_2.xml

[[Return to top](#)]

Agriculture Sector

20. *February 10, USA Today* — **Federal drill to test readiness for 'agroterror'.** Federal government leaders, including 18 members of Congress, are set to take part in a drill Tuesday to demonstrate what might happen if a terrorist attack were aimed not at humans, but at U.S. agriculture. The simulation, called Silent Prairie, taking place at the National Defense University, Fort McNair, will show how quickly and devastatingly an

outbreak of foot and mouth disease (FMD) could spread from state to state, affecting the national economy and psyche. Among those who will participate in the crisis simulation are Surgeon General Richard Carmona, Deputy Agriculture Secretary James Moseley, and representatives of the FBI and Federal Emergency Management Agency. No matter where it began, an outbreak "would not be a local event," says Thomas McGinn, assistant state veterinarian with the North Carolina Department of Agriculture, which has instituted a comprehensive plan to quickly detect and respond to agricultural terrorism. Because thousands of animals are transported across state lines every day, "any kind of foreign animal disease, if it took only five days to detect, would be all over the country," he said. **The goal of an attack on crops, farm animals, or food processors would be economic destruction, decreased faith in the safety of the food supply, food shortages, and the spread of disease, said veterinarian Paul Williams of Georgia's Emergency Management Agency. Rand Corporation analysts have reported that no U.S. city has more than a seven-day food supply on hand, he said, and "thousands of food processing plants have minimal biosecurity."**

Source: http://www.usatoday.com/news/nation/2003-02-10-agro-terror-d_rill_x.htm

21. *February 10, Agriculture.com* — **Meat groups protest proposed FDA restrictions on animal feed.** A coalition of agricultural organizations led by the American Meat Institute (AMI) is arguing that no scientific reason exists for the U.S. Food and Drug Administration's recent proposed changes to animal feed regulations. **In comments filed with FDA recently, the groups said safeguards are already in place to protect the U.S. livestock industry from the threat of bovine spongiform encephalopathy (BSE). In 2002, FDA published an Advanced Notice of Proposed Rulemaking (ANPR) seeking comments on proposed changes to the regulations that restrict the use of certain animal proteins from use in ruminant feed.** AMI has specifically expressed concern over FDA's suggestion that brains and spinal cords from ruminants two years of age and older be excluded from all rendered products. **In its comments, AMI said brains and spinal cords produced in the U.S. pose no BSE risk, and any regulations beyond those already in place would be redundant to existing animal feed regulations and could send the wrong message to other countries.** AMI is a national association that represents meat and poultry slaughterers and processors. Its members slaughter more than 90% of the cattle raised in the U.S. and process most of the rendered products produced in the U.S.

Source: http://www.agriculture.com/default.spb/AgNews.class?FNC=sideBarMore_ANewsindex.html_49333

[Return to top]

Food Sector

Nothing to report.

[Return to top]

Water Sector

22. *February 10, Water Tech Online* — **Water, wastewater facilities go to high terror alert.** The federal government on Friday raised the terrorist threat index for only the second time. "There

are no specific threats to water at this time," Rob Renner, deputy executive director of the American Water Works Association, told WaterTechOnline this morning. "As an association, we're taking this very seriously," he noted, saying facilities should be taking the time to be sure they have plans and contacts set up with their local law enforcement agencies and health agencies so they are prepared for any emergency. "We're encouraging utilities to practice even greater diligence," including reminding staff and contractors about the level-orange alert, and possibly increasing law enforcement surveillance of facilities. Source: <http://www.watertechonline.com/news.asp?mode=4font>>

23. *February 10, Globe and Mail* — **Drug traces found in cities' water. Trace amounts of prescription drugs have been detected in the drinking water of four Canadian communities.** This is the first time pharmaceutical products have been discovered in North America's municipal water supplies. The drugs were found through laboratory tests funded jointly by The Globe and Mail and CTV of water samples taken from 10 Canadian communities. The tests detected carbamazepine, an anticonvulsant given for epileptic seizures, in tap water from Montreal, Hamilton, and Brooks, a rural community in southern Alberta downstream of Calgary's sewage outflow. Another drug, gemfibrozil, used to reduce cholesterol levels, was found in Portage La Prairie, a Manitoba community known for farming and food processing. The tests found the drug residues in concentrations in the 6.5- to 70-parts-per-trillion range. One part per trillion is the equivalent of a grain of salt in an Olympic size swimming pool, and concentrations around this level are at the edge of what researchers can detect using modern laboratory equipment. **It is not known what health risk, if any, is posed by drinking or bathing in water containing trace amounts of drugs.** Source: http://www.globeandmail.com/servlet/ArticleNews/PEstory/TGAM/20030210/UWATEN/national/national/national_temp/5/5/8/

24. *February 10, New York Times* — **As cities move to privatize water, Atlanta steps back. Privatization has hit the water sector. Over the last five years, hundreds of American communities, including Indianapolis, IN, Milwaukee, WI, and Gary, IN have hired private companies to manage their waterworks, serving about one in 20 Americans. The main reason is that the cities are facing enormous costs to repair aging sewer pipes, treatment plants and other water infrastructure. Federal officials say the total cost of repairs could outstrip current spending by more than \$500 billion in the next 20 years. The utilities' hope has been that partnerships with private companies could generate savings and provide access to capital to help cover such staggering bills. But a cautionary tale has emerged in Atlanta, GA where the largest water privatization deal collapsed in January. Instead of public savings and private profit, a deal reached in 1999 between Atlanta and United Water resulted in bitter disappointments for all sides. Atlanta is now retaking control of a system that United Water was to have managed until 2019. The decision, in many ways, takes Atlanta back to square one. It will have a publicly controlled system that, on paper at least, will be more costly to ratepayers than the one it replaces. The arrangement offers no clear way to pay for extensive water-system repairs, estimated to cost \$800 million over the next five years. A separate bill to upgrade the city's sewers could exceed \$3 billion. The breakup comes as the question of privatized water is generating increased attention around the country, with advocacy groups like Public Citizen waging campaigns against the proposed deals. And while water privatization advocates describe the Atlanta failure as an aberration, all sides say that it is likely to weigh heavily in places like**

Stockton, CA, which is considering whether to go down a similar path. **"This is a huge setback for privatization, and it's going to have to give both cities and companies pause,"** said Dr. Peter H. Gleick, president of the Pacific Institute, a nonpartisan environmental research organization in Oakland, CA, that has written extensively about the risks and benefits of water privatization.

Source: <http://www.nytimes.com/2003/02/10/national/10WATE.html>

[[Return to top](#)]

Public Health Sector

25. *February 10, Philadelphia Inquirer* — **Scientists: bolster labs' security. Concern about bioterrorism have prompted Congress to pass laws restricting access to U.S. labs that handle dangerous biological agents, but some scientists say the new rules don't go nearly far enough to keep those labs secure.** The level of security still varies widely among labs, and some researchers say the new rules won't change that. The fuzziness about security manifests itself as a dangerous biological agent makes its way from one lab to another. At some points security seems minimal; at others, overwhelming. Last summer, for instance, a package for microbiologist Nancy Connell arrived without fanfare by FedEx. The driver handed the package to loading dock workers at the Newark campus of the University of Medicine and Dentistry of New Jersey. No police were at the scene to ensure the package was put in the proper hands. Once Connell carried the package to her lab, the security level changed dramatically. Connell needed a coded key card to open three doors. Surveillance cameras recorded her every move. Then, using another code, the researcher entered an inner lab. Inside the package was a vial of the bacteria *Yersinia pestis* or the plague. Others say the real threat comes not from shipment of biological agents or from outsiders breaking into a lab, but from those who already have valid access. **Researchers and university officials do not view theft from the outside as a major risk. Kenneth J. Soprano, Temple's vice president for research, says: "What people have to fear is not someone coming in off Broad Street. Typically, if someone came into my lab looking for anthrax, they'd never be able to find it. But a disgruntled postdoctoral student would have no problem finding it, plus the key to the freezer. All the legislation in the world won't change that."**

Source: <http://www.philly.com/mld/inquirer/news/front/5144876.htm>

26. *February 10, Sydney Morning Herald* — **UK tests technology that warns of terror attack. The British government is looking at buying equipment which could provide mobile early warnings of a biological attack by terrorists. The equipment, about the size of a large refrigerator, could be installed in vans to provide mobile detector units.** Officials are testing units called NB Cerberus, built by a British firm, which can detect deadly viruses, toxins, or bacteria released in a terror attack. The units could then be used at any public event where thousands of people gather, such as sporting events or concerts to give early warning of an attack from anthrax, smallpox, or ricin. **The units are being tested at Porton Down, the government's chemical weapons centre in Wiltshire. It is thought when the tests are completed, in about nine months time, the government will place an order to boost the UK's defenses.** The Ministry of Defence is currently buying 20 new IPBS, Integrated Biological Detection Systems, mounted on four-ton trucks and used by the military to give an early warning of bio-attacks on the battlefield. The new equipment's full name is Nuclear,

Biological and Chemical Cerberus.

Source: <http://www.smh.com.au/articles/2003/02/10/1044725717900.html>

[[Return to top](#)]

Government Sector

27. *February 10, Associated Press* — **Ridge says latest warning most serious.** Homeland Security Secretary Tom Ridge said Monday the latest terrorism alert issued by the Bush administration represented "the most significant" such warning since the Sept. 11, 2001 attacks. **"One of the reasons that we raised it is that because we believe the threat has substantially increased in the last couple of weeks,"** Ridge said on CBS's "The Early Show." **The administration last Friday, citing intelligence that it said suggested a growing threat from Osama bin Laden's al-Qaida terrorist network, increased the level of alert from yellow to orange.** Ridge was questioned about the seriousness of the warning, which remains in effect. "In discussing this matter with people that have been around the White House longer than I have, it is universally agreed that this is the most significant set of warnings that we've had since before Sept. 11," he replied. **Appearing on NBC's "Today" program, Ridge said the warning was based on "the accumulation of credible corroborated sources, none of which are connected to the possibility of military involvement with Iraq." Ridge, however, said it was not possible to be more specific about possible targets.** "We get general information and specific information, but none of the specific information talks about time, place or methods or means ... We don't get the specificity that we would all like to have in order to prepare," he said.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A51057-2003Feb 10.html>

28. *February 10, Washington Post* — **Congress hopes to raise FBI funding to \$4.3 billion.** House-Senate negotiators who are close to completing a compromise version of the huge spending measure have agreed to provide nearly \$4.3 billion to the FBI, about \$45 million more than President Bush had sought, congressional sources said. Senior House members in both parties say they are pleased with FBI changes begun in the past year. The White House appears to share that confidence. **Last week, it sent a strong signal of support for the bureau when it announced its 2004 budget proposal, which includes an increase of nearly 10 percent for the FBI, to \$4.6 billion. The extra money would pay for more than 1,900 new positions at the bureau, including more than 800 analysts and surveillance officers and hundreds of agents devoted to counterterrorism and counterintelligence.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A49027-2003Feb 9.html>

29. *February 07, Department of Homeland Security* — **Agency actions in response to the national elevated alert level .** On Friday, Secretary Ridge and Attorney General Ashcroft announced that the national alert level is being raised from Yellow (Elevated Risk) to Orange (High Risk). As a result, many agencies that will be a part of the new Department of Homeland Security on March 1, are taking additional steps to increase their protective measures. **Following are a few examples of additional steps being taken by some of these agencies. These are provided as representative examples, and should not be construed as the complete Federal response to the increased threat level.** Border and Transportation Security Directorate Transportation Security (Transportation) – Transportation Security

Administration (TSA) screeners will increase the number of random examinations conducted at airport security checkpoints. Federal Air Marshals will be assigned to a greater number of flights. **Customs (Treasury), Immigration (Justice) and APHIS (Agriculture) Passengers** – Customs, Immigration and Agriculture inspectors will be questioning more people more closely as they cross the land border, or enter the United States through international airports. **Cargo** – Customs inspectors will increase the number of cargo containers and trucks that they identify for additional screening with non-intrusive inspection equipment. **Between Ports of Entry** – The Border Patrol's Special Response and Border Search and Rescue teams nationwide have been placed on standby and are prepared to deploy to address specific threats as necessary. **Federal Protective Service (GSA)** – FPS will increase security at Federal Buildings by performing additional checks of hand carried items and by increasing random searches of vehicles. **Emergency Preparedness and Response** – FEMA is in regular contact with security Points of Contact to collect and disseminate threat and intelligence information. **Office of Energy Assurance** – Establish daily contact with industry to share information. Review plans for and be prepared to immediately implement SEVERE (Red) Threat Condition measures. **U.S. Coast Guard** – The U.S. Coast Guard is increasing its patrol operations with cutters, aircraft and boats, and is closely monitoring maritime activity. **U.S. Secret Service** – While the vast majority of steps are not observable to the general public, the U.S. Secret Service is and remains at a heightened state of alert.

Source: <http://www.dhs.gov/dhspublic/display?content=452>

[Return to top]

Emergency Services Sector

30. *February 09, Washington Post* — **Terrorism drill moves fears closer to home.** Saturday's massive exercise at U.S. District Court was national news, complete with media staging areas and "guidelines for coverage." Coming just one day after the government raised the terrorist threat alert to the second-highest level, hordes of reporters and politicians huddled outside the courthouse in the frigid morning air, where a tanker truck from "Mike's Tanker Rental" had been flipped onto the snowy ground. **The exercise was designed to help myriad agencies work together and assess their readiness, officials said. Among those participating were Alexandria police and fire departments, the FBI, the Virginia Department of Emergency Management, the U.S. Marshals Service and the U.S. Marine's Chemical Biological Incident Response Force. Special gas masks and other high-tech equipment purchased after the Sept. 11 terrorist attacks were also put to the test.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A45713-2003Feb 8.html>

31. *February 07, Federal Bureau of Investigation* — **Seeking information on Mohammed Sher Mohammad Khan.** The Federal Bureau of Investigation is seeking the public's assistance in determining the whereabouts of the following individual: **Mohammed Sher Mohammad Khan, Alias: Muhammad Shir Muhammad Khan; Mohammed Essagh; Ja'Far Al-Tayar; Jaffar Tayar; Jaafar Al-Tayyar; Ali Abdul Qadir; Abdul Qadir** Date of Birth: November 11, 1966; Place of Birth: Swat, Pakistan Height: 5'3" to 5'7" Weight: 132 pounds Hair: Black Eyes: Black **The above individual, whose name and date of birth may be fictitious, is believed to have entered the United States illegally after September 1, 2001. Khan is an English speaker and sometimes has a beard. He is also asthmatic. Although the FBI has**

no specific information that this individual is connected to any potential terrorist activities, based upon information developed in the course of on-going investigations, the FBI would like to locate and question this person. The FBI has been working with Homeland Security Agencies (U.S. Customs, INS, TSA) to locate this individual. The above information has also been disseminated to the appropriate law enforcement agencies around the United States and throughout the world.

Source: <http://www.fbi.gov/pressrel/pressrel03/mueller020703.htm>

[[Return to top](#)]

Information and Telecommunications Sector

32. *February 07, Medill News Service* — **Don't underestimate cyberterrorists, experts warn.**

The Internet is becoming a new battleground for warfare, according to experts concerned about the potential of a cyberattack to cripple the public infrastructure. The recent Slammer worm, which blocked Internet traffic and crippled some corporate networks for most of a weekend, is just a watered-down version of a cybercrisis that could disrupt everything from banks to water supplies, critics say. In the Mideast conflict, pro-Palestinian hackers have successfully taken down Web sites of the Israeli Parliament, the Israeli Defense Force, the Foreign Ministry, the Bank of Israel, the Tel Aviv Stock Exchange, and others, according to a report by Dartmouth College's Institute for Security Technology Studies. Dartmouth's study charts how **political cyberattacks often precede physical attacks. Cyberattacks after U.S.-led military action are "extremely likely" and could possibly be catastrophic,** according to the report. **Information systems—like electrical infrastructures, water resources, and oil and gas—should be considered likely targets, it warns. While cyberattacks can take a variety of forms and may originate from terrorist groups or targeted nation states, they are more likely to be launched by sympathizers or thrill-seekers,** according to the institute's report.



Source: <http://www.idg.net/go.cgi?id=785058>

33. *February 05, CNET News* — **GSA pulls suspicious .gov site.** The General Services Administration (GSA), which runs the .gov registry, pulled the plug on a .gov Web site pending an investigation into the authenticity of the organization that controlled it. Until January 24, the AONN.gov Web site contained information about an agency calling itself the Access One Network Northwest (AONN), a self-described cyberwarfare unit claiming to employ more than 2,000 people and had the support of the U.S. Department of Defense. No federal agency called AONN appears to exist, and no agency with that name is on the official list of organizations maintained by the U.S. National Institute of Standards and Technology. **The action could point to the first case of a .gov domain name hijacking.** Cybersquatting, or registering a domain to which you may not be entitled, is hardly uncommon among the multitude of .com and .net domains. But there are no known cybersquatting incidents involving a governmental domain, according to the GSA. Claiming credit for the deleted .gov site is a man who calls himself Robert L. Taylor III. Taylor declined to explain how or when he secured a .gov domain for the group, calling AONN's operations "classified." **A Pentagon representative said that AONN has no affiliation with the U.S. military and he had no knowledge of the organization.** According to the official .gov registration rules, only organizations that appear in an official list of government agencies qualify for a .gov

domain—and AONN is not on it. Registering a .gov domain name involves writing an authorization letter, printing it out, and then sending it to the ".GOV Domain Manager" in Reston, Virginia.

Source: http://news.com.com/2100-1023-983384.html?tag=fd_ots

Internet Alert Dashboard

Current Alert Levels	
 <p>AlertCon: 1 out of 4 https://etoc.iss.net</p>	 <p>Security Focus ThreatCon: 1 out of 4 www.securityfocus.com</p>
Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: PE_FUNLOVE.4099 Source: http://wtc.trendmicro.com/wtc/wman.html , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	137 (netbios-ns), 1434 (ms-sql-m), 80 (http), 53 (domain), 1433 (ms-sql-s), 445 (microsoft-ds), 139 (netbios-ssn), 21 (ftp), 443 (https), 25 (smtp) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

[Return to top]

General Sector

34. *February 10, Newsweek* — **What's behind latest "Orange Alert"**. The Bush administration raised the national threat alert from "yellow" to "orange" Friday after **receiving new intelligence reports that pointed to the possibility of multiple imminent attacks by al Qaeda against Jewish groups and Jewish-owned businesses inside the United States, Newsweek has learned.** Acting swiftly on the reports, FBI officials began contacting Jewish leaders and rabbis around the country Friday to warn them to be especially vigilant and to enhance security at Sabbath services and other events over the weekend, law-enforcement sources said. State and local police were also being asked to provide extra patrols for Jewish religious services and other gatherings. Officials said the new intelligence warned about the possibility of attacks on synagogues, Jewish community centers, Jewish hospitals, youth groups, hotels and resorts. **Law-enforcement officials stressed that they had no information that could help them identify any specific targets and that it was difficult to stress the credibility of much of the intelligence reporting. But officials said they were unusually worried both because of recent electronic intercepts, both inside the United States and overseas that "strongly suggests" an imminent attack as well as the sheer volume of reports mentioning Jewish targets that came in over the last few days.** This is a full-court press, said one FBI official about the bureau's sudden outreach to Jewish groups. There's real anxiety about this. A senior law-enforcement official said the volume of threats relating to

Jewish interests inside the United States was a major factor in prompting President Bush to raise the intelligence threat level to orange, which is the color code for a high risk of terrorist attack.

Source: <http://www.msnbc.com/news/870219.asp?ocv=CB10>

35. *February 10, New York Times* — **A terrorist with a deadly past.** A Jordanian of Palestinian ancestry, Abu Mussab al-Zarqawi followed a now-familiar path of political alienation and religious fervor to militant causes. He was largely unknown to most Americans until last week when Secretary of State Colin L. Powell, in his presentation to the United Nations, singled him out as the most important link between Iraq and Al Qaeda. Powell told the United Nations that Zarqawi had set up a terrorist cell in Baghdad and that he was affiliated with Ansar al-Islam, a small militant group in northern Iraq that Americans say has ties to al Qaeda. Kurdish officials today accused the group of assassinating a government official on Saturday. **Interviews with intelligence officials in the United States and Europe, along with a report prepared by the German authorities, indicate that Zarqawi has a long history of terrorism and has engineered a number of deadly acts. Most recently, the authorities said several of his associates shot to death Laurence Foley, an American diplomat in Jordan, last Oct. 28. Officials agree that Zarqawi, 36, is a charismatic terror lieutenant whose dual specialties chemical weapons and recruitment make him a potent and dangerous force. But there is less consensus about Powell's contention that Zarqawi exemplifies a fledgling alliance between Iraq and al Qaeda.** The loss of a limb apparently did not diminish his fierce passion to construct a network of terrorists throughout Europe, according to American and European intelligence officials. Powell said Zarqawi had settled in Baghdad last year and began to establish a terror network whose ambitious goal was to carry out attacks using chemical weapons in Britain, France, Spain, Italy and Russia. **Zarqawi's group is known as al Tawhid, which Powell described as an "affiliate" of al Qaeda whose terrorist goals seemed indistinguishable from those of Osama bin Laden's network.**

Source: <http://www.nytimes.com/2003/02/10/international/middleeast/10TERR.html>

36. *February 09, Los Angeles Times* — **Amateurs' may join in terrorism.** A U.S. war with Iraq could sharply escalate a growing and hard-to-disrupt variant of international terrorism: sudden assaults by sympathizers acting alone or in small groups and motivated by religious fervor, U.S. and allied counter-terrorism officials say. Atty. Gen. John Ashcroft warned the nation Friday of renewed threats by Osama bin Laden's Al Qaeda network, publicly insisting that a recent spike in activity by terror cells around the globe is unrelated to the increasing likelihood of a military showdown with Iraq. **Privately, however, U.S. counter-terrorism authorities and their counterparts overseas said that there is a connection, and that Al Qaeda cells are thought to be planning attacks against Americans and other Westerners as a show of solidarity with Muslims in Iraq. Citing recent intelligence, these authorities also fear that a potential second front in the war on terrorism is taking shape. A groundswell of anger toward the United States, they said, could prompt attacks by Muslims with no formal ties to terrorist organizations — in response to what they view as an assault on Islam.** "These are amateurs who are mobilized by the rhetoric, who take it upon themselves to go on missions and cause terrorism upon unprotected targets that are a symbol of their hatred," said Magnus Ranstorp, a counter-terrorism consultant to several European governments.

Source: <http://www.latimes.com/news/printedition/la-na-terror9feb09001509.1.3580452.story>

37. February 09, Associated Press — **Secret papers stored in basement.** National Guard intelligence officer Rafael Davila admits he spent years bringing home secret and top-secret documents, stacking them in his basement and finally in a rented storage locker. He told the FBI he just wanted to read them. **Prosecutors have accused Davila and his ex-wife, Deborah, of espionage. Investigators are still trying to track down hundreds of files apparently containing information about nuclear, chemical and biological warfare. A federal indictment charges the Davilas with unauthorized possession of sensitive documents during the first eight months of 1999. Deborah Davila is also charged with trying to deliver the documents to an unidentified person in August of that year.** During a hearing this week, Davila, 51, sat silently with Deborah, 40, as prosecutors vilified them for allegedly exposing the nation to danger from terrorists and anti-government extremists.
Source: <http://www.washingtonpost.com/wp-dyn/articles/A45214-2003Feb8.html>

[Return to top]

NIPC Products & Contact Information

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the NIPC web-site (<http://www.nipc.gov>), one can quickly access any of the following NIPC products:

NIPC Advisories – Advisories address significant threat or incident information that suggests a change in readiness posture, protective options and/or response.

NIPC Alerts – Alerts address major threat or incident information addressing imminent or in-progress attacks targeting specific national networks or critical infrastructures.

NIPC Information Bulletins – Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.

NIPC CyberNotes – CyberNotes is published to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

NIPC Daily Open Source Report Contact Information

Content and Suggestions:

Melissa Conaty (202-324-0354 or mconaty@fbi.gov)

Kerry J. Butterfield (202-324-1131 or kbutterf@mitre.org)

Distribution Information

NIPC Watch and Warning Unit (202-323-3204 or nipc_watch@fbi.gov)

NIPC Disclaimer

The NIPC Daily Open Source Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal NIPC tool intended to serve the informational needs of NIPC personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The NIPC provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.

Jonathan B. Mullin, 10:23 AM 2/9/2003 -0500, Fwd: FW: Advisory #1, R4 ROC Activation

X-Sender: jmulin@mail.hq.nasa.gov
X-Mailer: QUALCOMM Windows Eudora Version 4.3.2
Date: Sun, 09 Feb 2003 10:23:23 -0500
To: HCAT@hq.nasa.gov
From: "Jonathan B. Mullin" <jmulin@hq.nasa.gov>
Subject: Fwd: FW: Advisory #1, R4 ROC Activation
Cc: a.h.phillips@larc.nasa.gov, aodonogh@hq.nasa.gov, alee@hq.nasa.gov, bdoici@arc.nasa.gov, cathy.miller@msfc.nasa.gov, tsabikos.a.papadimitris.1@gsfc.nasa.gov, chunt@mail.arc.nasa.gov, clyde.dease@ssc.nasa.gov, dhall@wstf.nasa.gov, Eric.G.Fuller@jpl.nasa.gov, Ezra.R.Abrahamy@jpl.nasa.gov, frederick.w.battle.jr@jpl.nasa.gov, h.w.beazley@larc.nasa.gov, jack_vechil@mail.dfrc.nasa.gov, dennis.g.perrin1@jsc.nasa.gov, luequention.wilkins@grc.nasa.gov, lengelbert@mail.arc.nasa.gov, michael.moore@maf.nasa.gov, probles@nmo.jpl.nasa.gov, sonja.alexander@hq.nasa.gov, stephen.a.turner@maf.nasa.gov, terry.m.potterton.1@gsfc.nasa.gov, tom.ambrose@dfrc.nasa.gov, wayne.kee-1@ksc.nasa.gov, Robert.Turner@hq.nasa.gov, howard.kass@hq.nasa.gov, alee@hq.nasa.gov, william.barry-1@ksc.nasa.gov, odomingu@hq.nasa.gov, Catherine.Angotti@hq.nasa.gov, mmcneill@mail.hq.nasa.gov, tspagnuo@pop200.gsfc.nasa.gov, Patrick.A.Hancock.1@gsfc.nasa.gov, Jim.Carter@msfc.nasa.gov, Edwin.Jones@msfc.nasa.gov, john.rodgers@hq.nasa.gov, bnotley@mail.arc.nasa.gov, gregory.l.ellis.1@gsfc.nasa.gov, t.f.middleton@larc.nasa.gov, william.c.roeh1@jsc.nasa.gov, phillip.j.nessler.1@gsfc.nasa.gov, pete.allen@msfc.nasa.gov, jlabrecq@hq.nasa.gov, cherbert@hq.nasa.gov, astowes@hq.nasa.gov, Ernest.M.Graham@msfc.nasa.gov, dan.thomas@hq.nasa.gov, g.m.watson@larc.nasa.gov, rdilustr@mail.hq.nasa.gov, hstewart@hq.nasa.gov, speyton@hq.nasa.gov, jlemke@hq.nasa.gov, whill@hq.nasa.gov, michael.stevens-2@ksc.nasa.gov, jlloyd@hq.nasa.gov, prichard@hq.nasa.gov, robert.t.gaffney1@jsc.nasa.gov, james.o.cheek@usago.ksc.nasa.gov

For your information only, FEMA advisory. Regards, Jon

From: FEMA OPERATIONS CENTER <FEMA.OPERATIONS.CENTER@fema.gov>

To: EST-DIR <EST-DIR@fema.gov>, Action Officer <ActionOfficer@fema.gov>,
"ARNGOPS (E-mail)" <ARNGOPS@ngb.army.mil>,
BBS Submissions

<BBSSubmissions@fema.gov>,
Blystadt <blystadt@usa.redcross.org>,
"D'Araujo, Jack" <Jack.D'Araujo@fema.gov>,
"Debbi Yamanaka (E-mail)"

<dyamanaka@arrow-mountain.com>,
"DOMS (E-mail)" <foxhole@doms.army.mil>,
"DOT OPS - 1 (E-mail)" <tioc-01@rspa.dot.gov>,
"Edward Massimo (E-mail 2)" <Edward.C.Massimo@HQ02.USACE.ARMY.MIL>,
"EPA-EOC HQ (E-mail)" <EOC.EPAHQ@epa.gov>,
"ESF-08 HHS Jevac (E-mail 2)"

<rjavec@osophs.dhhs.gov>,
FEMADESKREPS <FEMADESKREPS@fema.gov>,
"GSA Montgomery (E-mail)" <kathy.montgomery@gsa.gov>,
"HUD McCarthy (E-mail)" <bruce_e._mccarthy@hud.gov>,
"HUD Opper (E-mail)"
<jan_c._opper@hud.gov>,
"James Lloyd (E-mail)" <JLloyd@hq.nasa.gov>,
"Jonathan Mullin (E-mail)" <JMullin@hq.nasa.gov>,
"Karen Maguire (E-mail)" <karen.maguire@usda.gov>,
Mary Margaret Walker
<Mary.Margaret.Walker@fema.gov>,
"Maryan Chirayath (E-mail)"
<maryan.chirayath@bea.gov>,
Michael Mascaro <michael.mascaro@bea.gov>,
"NCS (E-mail)" <NCS@NCS.GOV>,
"Nieuwejaar, Sonja"
<Sonja.Nieuwejaar@fema.gov>,
"Nmci (E-mail)" <NMCICommandCenter@eds.com>,
"Paolin Hatch (E-mail)" <paolin.hatch@gsa.gov>,
"Parkes, Rose"
<Rose.Parkes@fema.gov>,
"USACE Acosta (E-mail)"
<louis.a.acosta@HQ02.USACE.ARMY.MIL>,
"USACE Aguilera (E-mail)"
<karen.durham-aguilera@usace.army.mil>,
"USACE Gilmore (E-mail)"
<george.l.gilmore@usace.army.mil>,
"USACE Hecker (E-mail)"
<edward.j.hecker@usace.army.mil>,
"USACE Irwin (E-mail)"
<william.e.irwin@usace.army.mil>,
"USACE Miller (E-mail)"
<lizabeth.h.miller@usace.army.mil>,
USACE OPS <ce-uoc@usace.army.mil>

Subject: FW: Advisory #1, R4 ROC Activation

Date: Sun, 9 Feb 2003 10:09:41 -0500

X-Mailer: Internet Mail Service (5.5.2656.59)

> -----Original Message-----
> From: Aadnesen, Paul
> Sent: Sunday, February 09, 2003 9:33 AM
> To: R4-Advisory-List
> Subject: Advisory #1, R4 ROC Activation
>
> <<Advisory1.doc>>

Jonathan B. Mullin
Manager Operational Safety