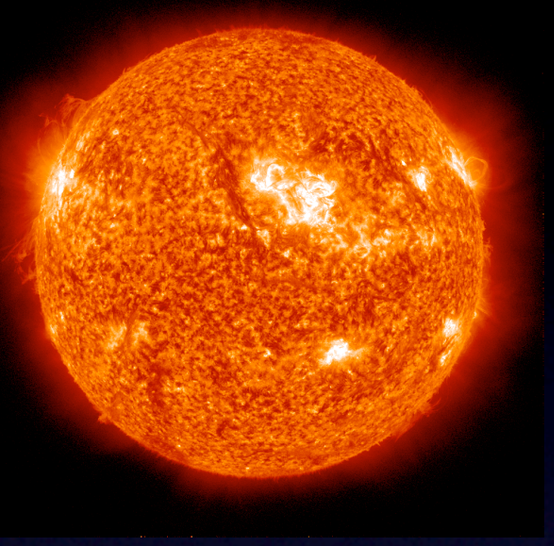
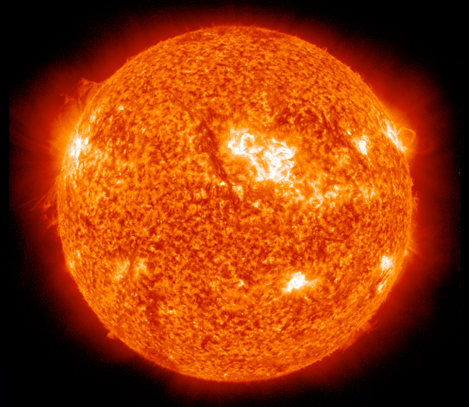


Working with Code 700

A Worm's-Eye View

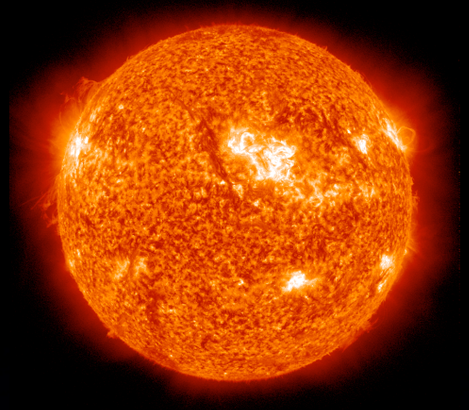
Joe Gurman
Solar Physics Laboratory, Heliophysics Science Division

2011 September 20



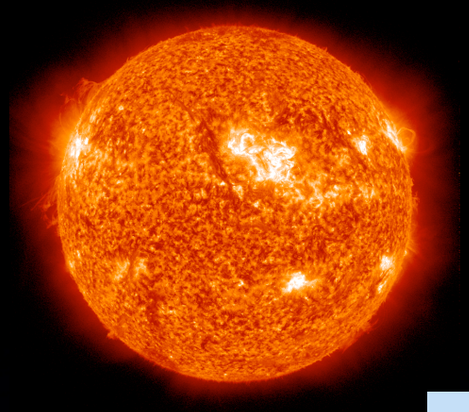
Disclaimers

- This is truly a worm's-eye view
  - Deals only with *SOHO*, STEREO Science Center (SSC), and Solar Data Analysis Center (SDAC) experiences with various parts of Code 700
- All statements and opinions are those of the author and no one else



The Good, the Bad, and the Ugly

- The Good: Any technical function
- The Bad: Any management function
  - Long history of not communicating changes in requirements but assuming we have to respond to those changes – while in most cases we hear about the changes when they ball us out for not complying
- The Ugly
  - Management that insists on meticulous adherence to trivial but onerous Agency requirements, but apparently feels free to ignore the requirements whenever they chose
    - Unlikely that this is a conscious decision, but instead reflects an organization responding to serious, outside pressure to produce results in a fixed time frame



Which parts of 700?

Information Technology & Communications Directorate(ITCD)

Information Technology & Communications Directorate
Code 700

Adrian Gardner, Director and CIO
Dennis Vander Tuig, Deputy CIO for Enterprise Solutions

Laverne Dickens, Assoc. Director Business & Planning
(IT Service & Quality Manager)
Lon Gowen, Assoc. Director for Innovation
Car Johnson, Assoc. Director for Enterprise Integration
Bradford Torain, Associate Director for Operations
Myra Bambacus, Senior Advisor
Tonjua Hines-Watts, Center Enterprise Architect
Josh Krage, Center Chief Information Security Officer
Deborah Sharpe, IT Governance
IT Managers
Natalie McMurdy, Administrative Officer

Strategy & Planning Office
Code 702
E. Joseph Stevens, Chief
Paul Hunter, Associate Chief

Business & Investment Management Office
Code 703
David Baden, Chief
Vacant, Assoc. Chief

Program Integration & Management Division
Code 740
Michele Woctenfuss, Chief
Amy Fedorchak, Associate Chief

Enterprise Solutions Division
Code 750
Dwaine Kronser, Chief
Tamra Goldstein, Associate Chief
Stephen Naus, Assistant Chief

Communications & Security Services Division
Code 760
Keith Keller, Chief
Margarita Penn, Associate Chief

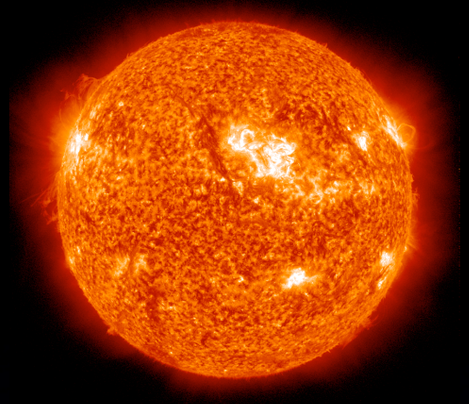
Communications Services Branch
Code 761
Sergio McKenzie, Branch Head

Engineering & Security Services Branch
Code 762
Matt Kirichok, Branch Head

WFF IT & Communications Branch
Code 763
Scott Webb, Branch Head

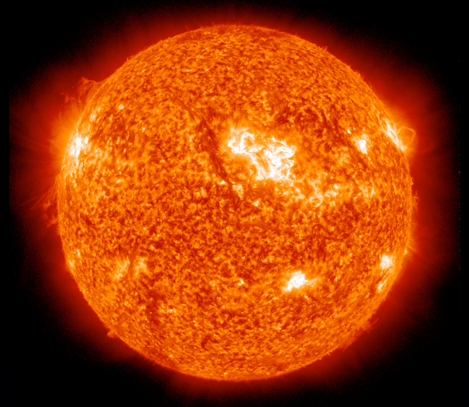
-Chart updated June 16, 2011

Point of contact: Natalie McMurdy
Natalie.McMurdy-1@nasa.gov
Content Owner: Dennis Vander Tuig



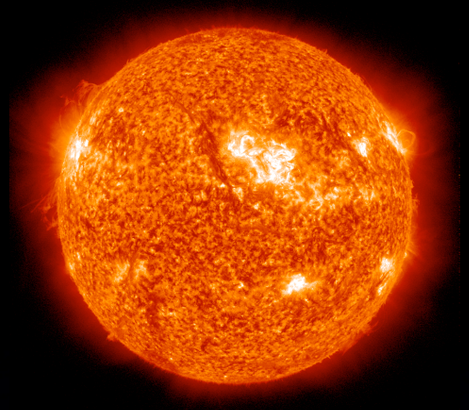
The Good (I)

- Majordomo to Agency mailing lists transition (740): smooth
- History of support for solar missions by GCC (IONet; 760): superb
  - *SOHO*, STEREO, SDO
  - SDO data distribution: engineered dedicated network for us to for SDO data caching, distribution; going to 2 Gbps Friday, 09•23
    - Probably understaffed, but extremely responsive to user requirements
    - Virtually no formal process: just identify requirements, have them study, identify funding source, and they execute



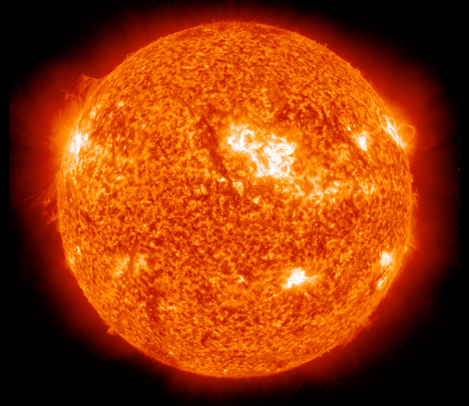
The Good (II)

- Day-to-day security (762)
  - extremely responsive
    - react within minutes to hours to any perceived anomaly
  - Also provide management of "our" firewall, switches at no recurring cost
  - Management keeps us informed, on an ongoing and *informal* basis, of at least some changes in requirements



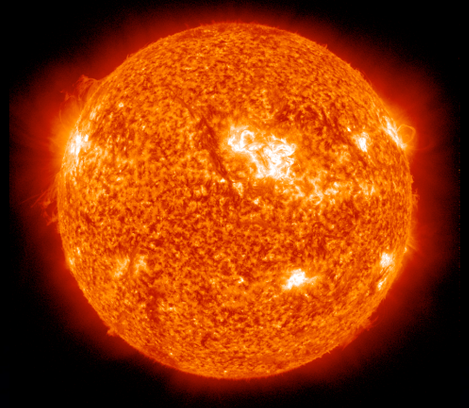
The Good (III)

- Innovation (Lon Gowen/700)
  - Took time to explain "innovation" cloud personally
  - Again took time help us examine whether that cloud was appropriate for Helioviewer application
  - Had a responsive quote for reliable hardware for primary Helioviewer service available within 48 hours



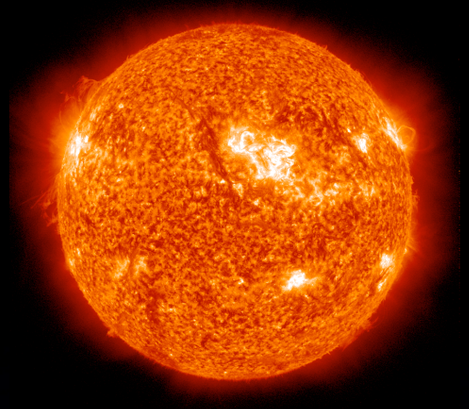
The Good (IV)

- SEWP (703)
  - The "anti-ODIN (ACES)"
    - one size does *not* fit all, but by being inclusive, can achieve cost savings while providing federal customers with the IT commercial, off-the-shelf (COTS) products they need to meet their requirements
  - Also saves 600 personnel an enormous amount of paperwork and delay in procuring COTS IT products
    - Since the inaptly named NASA "Competitiveness Council" ukase of 2007, we need a waiver from ODIN purchasing in order to use SEWP: just plain silly



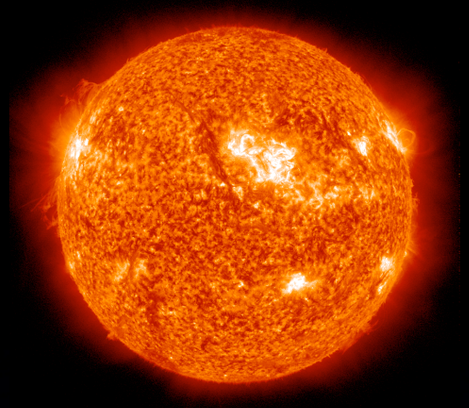
The Bad (I)

- From our lead SA (regarding IONet/GCC):
  - "Communication, communication, communication, or the lack thereof"
    - Institutional history (dates to pre-700) of not communicating changes and requirements down to the ISSO/SA level
    - ....but assuming they are somehow known
    - Could use a weekly digest of changes and/or an IONet +CNE/SAs mailing list



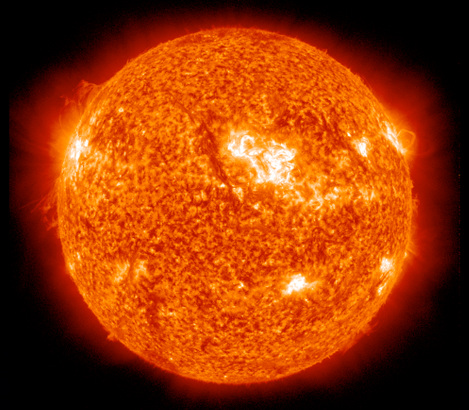
The Bad (II)

- Regarding the NDC (CNE)
  - SA receives multiple spreadsheets of vulnerabilities each month, though which she must search to see if any of our machines are affected
  - Once again, a digest or notification to the SA of the affected machine(s) would result in much more efficient use of our SAs' time
    - Our SAs are not interchangeable parts; they are extremely knowledgeable, experienced, and critical personnel for our missions/projects who represent living archives of mission configuration and requirments



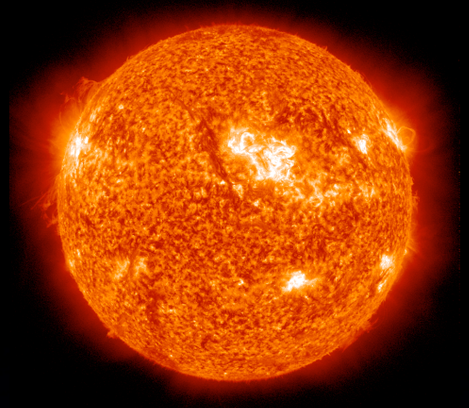
The Ugly (I)

- We are a special case: our own C&A "system"
  - Mostly on another network, but 600 assets rather than 400
  - Decision driven by risk management consideration
- Consequences of decision
  - ~ 1/3 of lead SA's time is spent on C&A-related activities of little obvious value to missions
    - Not what we hired her for
  - Constant requirement change/gallop
  - Trivialization of process
    - "Low" sensitivity system audit is a (bad) joke



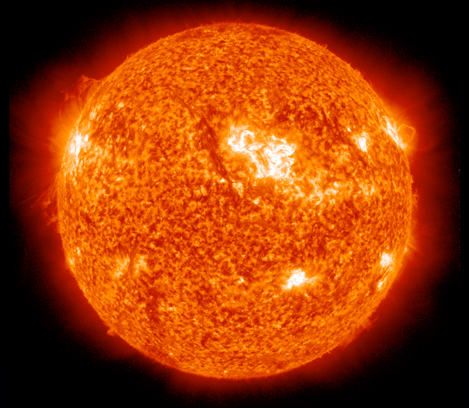
The Ugly (II)

- C&A "process" (continued)
  - ATO delayed for > 3 months because a secretary didn't like the signature page
- We could have lived with all of the above, but....
  - IG report on "mission networks" vulnerabilities identified 6 vulnerable systems (4 no longer in use or not connected to the Internet)
  - In conjunction with the White House, Agency response was to initiate penetration testing using DoE pen test team
  - And then our issues began....



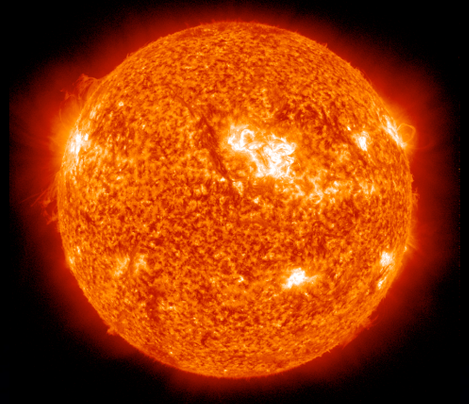
The Ugly (III)

- Penetration testing (continued)
  - Originally informed by 703 personnel of types (external, internal) of testing and protocols
  - We responded with willingness, but pointed out that internal, "credentialed" testing would require waiving of "common controls" in our C&A plans
    - 703 personnel derogatorily referred to our concerns as "dotting the i's and crossing the t's), even after we explained that otherwise, we were simply failing a social engineering pen test, but agreed to have Center CIO provide authority
      - Note: Not clear, under 7120.5, that Center CIO has this authority for operating mission systems, but we wanted to comply and welcomed the opportunity for pen testing



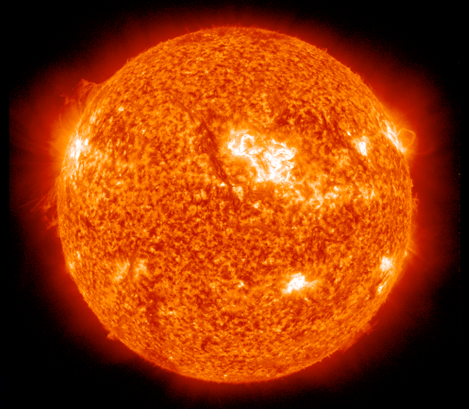
The Ugly (IV)

- Penetration testing (continued)
  - Non-credentialed pen testing carried out from within our network
    - DoE personnel provided full information on results
  - Suddenly, 703 insisted on credentialed, internal pen testing of every system on our network (and similarly for all projects in scope) to meet early October deadline to report back to White House
    - Insisted on *same privileged username and password on all systems*
    - We refused
    - ....as did everyone else



The Ugly (V)

- Penetration testing (continued)
  - Current plan is to have a limited number of public-facing systems (*e.g.* Web and ftp servers) tested in this manner
    - We are still refusing to offer identical username-password combinations for credentialed testing
    - ....but certainly agree with making testing possible
  - External pen testing purportedly ongoing or going to occur within next few weeks (DoE team availability)
- Trying to be as charitable as possible:
  - Appears to be relatively inexperienced person in coordination role
  - But why chose that person?



The Ugly (VI)

- More serious concerns
  - Based on a telecon last week
  - Center CIO's office appears willing to buy into a particular security approach because it's recommended by the vendors of that approach
    - Difficult to credit, but that was actually given as the argument
  - Not clear the CIO organization is the right one for management of security for mission networks
    - Personnel are only now being sensitized to mission risk management
    - Concerns are valid but actions appear to be top-down, rather than mission requirements-driven