Roadmap for Actionable Space Weather Advisory Service
13 September 2012

I. Requirement: Provide Actionable Space Weather Advisories (ASWA) that can remediate space weather induced threats to the client's data center.

II. Objective: Provide several levels of services to the client for space weather threat remediation that change based on the threat level.

III. Implementation:

A. A <u>two-phase approach</u> will provide levels of service for the client data center's threat mitigation for events due to space weather.

1. The **first phase** will be a *Risk Alerts for Mitigation and Preparedness (RAMP)* system that issues general alerts in the form of watches when a space weather event threshold is crossed and the risk of a hazardous event has increased significantly. These alerts can be issued hours to days in advance, depending upon the physical process causing the alert. These alerts will contain advisory ("heads-up") information, including relevant background to the event and provide potential cause-effects short explanations. They will be provided directly to the client. The reported event threshold level is not fixed and can be set independently by the client.

> **WARNING**: is issued when a hazardous event is occurring, is imminent, or has a very high probability of occurring. A warning is used for very active conditions posing a threat to life or property.
> **ADVISORY**: is issued in active to very active conditions that may cause significant inconvenience, and if caution is not exercised, it could lead to situations that may threaten life and/or property.
> **WATCH**: is issued when the risk of a hazardous event has increased significantly, but its occurrence, location, and/or timing is still uncertain. It is intended to provide enough lead-time in active conditions so that those who need to set their plans in motion can do so.
> **ALERT**: is issued when an event threshold is crossed. It contains information that is available at the time of issue.

2. The **second phase** will be a *Space Weather Immediate Forecast Technology (SWIFT)* system that issues specific alerts in the form of advisories and warnings when active or very active conditions lead to a high probability of a hazardous event. These alerts can be issued minutes to an hour in advance, depending upon the data and model results that cause the alert. These alerts will contain advisory information to aid the client in decisions related to data center safety actions. They will be provided directly to the client.

B. The <u>content and format</u> of RAMP and SWIFT information is the following.

1. **RAMP**: Watch alerts will contain alert type (GMDCON, RADCON, COMCON), name, level (including color, NOAA scale, and Defense condition designators), short text background (cause of the event and expected start, peak, duration/end), short text advisory information for client systems, and access to graphical depictions of event. Alert format will in-

clude client notification via text/graphical messages delivered via automated server-to-server connections. In addition, dedicated websites, Twitter feeds, and email text messaging would be possible.

2. **SWIFT**: Advisory and warning alerts will contain alert type (GMDCON, RADCON, COMCON), name, level (including color, NOAA scale, and Defense condition designators), short text background (cause of the event and expected start, peak, duration/end), short text advisory information for client systems, and access to graphical depictions of event. Alert format will include client notification via text/graphical messages delivered via automated server-to-server connections. In addition, dedicated websites, Twitter feeds, email/phone text messaging, phone calls, and expert consultations would be possible.

Geomagnetic Disturbance Condition (GMDCON): occurs when excessive quantities of solar charged particles perturb the Earth's magnetic and electric fields. For example, power systems may experience voltage spikes and transformer loading, ranging from inconvenient fluctuations to catastrophic failure.
Radiation Disturbance Condition (RADCON): occurs when excessive quantities of solar energetic particles increase the radiation environment. For example, computer systems at high altitudes or high latitudes may experience single event upsets, ranging from inconvenient command alterations to catastrophic failure.
Communication Disturbance Condition (COMCON): occurs when excessive quantities of solar photons perturb the Earth's ionosphere. For example, communication and navigation systems may experience disruptions, ranging from inconvenient degradations to catastrophic failure.

C. The scientific and operational legacy of providing RAMP and SWIFT information is the following.

1. **RAMP**: Watch alerts will be derived from Space Environment Technologies' (SET) operational systems deployed in support of U.S. Air Force and commercial aviation assets. Long-range operational Dst predictions will feed GMDCON alerts and are made with the SET Anemomilos algorithm; they range from under a day for extreme events to 5 days for smaller events. GOES and ACE satellite operational monitoring will feed the RADCON alerts; they range from minutes for extreme events to a few hours for smaller events. GOES and SDO satellite operational monitoring will feed the COMCON alerts; all forecasts are in the range of minutes and durations range from hours for extreme events to an hour for smaller events.
2. **SWIFT**: Advisory and warning alerts will be derived from combined Storm Analysis Consultants (SAC) and SET's operational systems deployed in support of client assets. Short-range operational electric field predictions will feed GMDCON alerts and are made with SAC algorithms; they range from under a minute for extreme events to minutes for smaller events. RADCON and COMCON alerts will be performed through the RAMP system.

Appendix A – Alert Scales

Scale Threat level	ASWA GMDCON	Threat Characteristics to Power and Data Center Systems
Extreme	GMDCON 1	Widespread voltage control and harmonic distortion problems can occur on the power grid; some grid systems may experience complete collapse or blackouts. Harmonics can be high enough to cause concern for damage to sensitive critical data center systems.
Severe	GMDCON 2	There may be possible widespread voltage control and harmonic distortion problems and some protective and critical load systems of customers may mistakenly trip out key assets.
Strong	GMDCON 3	Voltage corrections may be required and false alarms may be triggered on some protective devices.
Moderate	GMDCON 4	High-latitude power systems may experience voltage alarms and long-duration storms may cause transformer damage.
Minor	GMDCON 5	Weak power grid fluctuations can occur.

Appendix B – ASWA Project Workflow

A. Determine workflow requirements including alert types, actionable information, alert product delivery method, follow-up processes.
B. Develop RAMP and SWIFT ASWA alert products, obtain concurrence from client as to format and content, develop operational delivery system at TRL 6.
C. Validate against known historical storm conditions, and demonstrate operational prototype at TRL 7 to client.
D. Test and verify alert product transmission to client system at TRL 8.
E. Client delivery meeting (TRL 9) and training session.

Technology Readiness Levels (TRL)

TRL 1. Basic principles observed
TRL 2. Technology concepts formulated
TRL 3. Analytical proof-of-concept
TRL 4. Component validation in lab environment
TRL 5. Component validation in relevant environment
TRL 6. Model demonstration in relevant environment
TRL 7. System prototype demonstration in relevant environment
TRL 8. System complete, tested, and demonstration qualified
TRL 9. Successful operations

Appendix C – Testing, validation, verification protocols

A. Validate alert product content and format with client at early stage.
B. Validate automated, operational production process of alert products for a variety of quiet and storm conditions.
C. Validate geophysical accuracy of alert products against known storms.
D. Verify accurate and timely alert product transmission to client system.

Appendix D – SET Server Security

Computer systems security is of high importance for all SET projects and for SET's clients. The options SET uses for delivering data products to customers securely and cost-effectively are two-fold. In the past, the practice was to assign a ssh/scp/sftp username/password to clients, but this method is inherently insecure because a username and password can easily fall into the wrong hands and may allow access to other parts of a server. Two methods provide a means for server-to-server "pull" methods that protect both the server providing the data and the client/server retrieving the data: 1) Java servlets that operate in a secure "sandbox", and 2) MySQL access, which requires a username/password, but prevents other ways to access server/client operating systems. Both ensure clients are unable to gain access to any other part of the SET server besides the desired data subset. On the other hand, the customer controls their access by a direct link to a known server port so they can be assured of secure access on their side. Both options can be launched from within a program script at the customer's server; Java servlets are more extensible and versatile than MySQL access methods, and the latter are more cost-effective to develop and maintain. Another secure method for a client to "pull" data from a remote server is using the common http/HTML framework, but this method is very limited in functionality. If a client requires the highest security, MySQL is the preferred framework. If a client requires greater functionality, Java servlets is the preferred framework.