

# **StratML: The 2013 Boston Marathon Attack (Application Uses)**

**By R. Russell Ruggiero**

## **Introduction**

I want to make it clear from the start that the contents in this document would not likely have affected the outcome of the April 15, 2013 attack at the Boston Marathon. Rather it is an exploratory piece that is meant to provoke ideas and concepts that could help to thwart future attempts regarding this type of unfortunate event. Our hearts must go out to families and friends of the three killed and over two-hundred and sixty who were injured. We must also thank the people who attended to the dead and injured as a result of this cowardly incident. It is here where Strategy Markup Language (StratML), an open, machine-readable standard could possibly be leveraged to help reduce the loss of life and minimize injury regarding these types of “bombings” or “attacks”.

## **The Mandate**

Trying to create a seamless and agnostic Federal IT ecosystem would allow for improved bidirectional communication flow between agencies in dealing with manmade (e.g., oil spills, terrorist attacks, etc.) and natural (e.g., earthquakes, hurricanes, etc.) catastrophic events. Accordingly, taking the open-standards route will help get there from a technology interaction and, or coexistence point of view. In relation to the public sector, it will be open, machine-readable solutions like StratML that will help reach the goals of important initiatives like the Government Performance and Results Act (GPRA). Case in point: StratML could enable entities comply with section 10 of the GPRA Modernization Act (GPRAMA), particularly now that Office of Management and Budget (OMB) M-13-13 has reiterated the direction previously set forth in Circular A-119 to use voluntary consensus standards whenever possible.

## **An Agnostic Approach**

From a pragmatic viewpoint, building to open-standards (e.g., OASIS, W3C, ANSI, etc.) helps to promote an agnostic IT landscape. While a long and arduous process the open-standards route seems to be the logical path in deploying large-scale IT solutions. For example, StratML Parts 1 and 2 are American (ANSI) national standards and Part 1 has been approved as an international (ISO) standard. Hence, promoting a true agnostic environment for interested parties and leverage the numerous strategic planning capabilities of StratML.

## **StratML Summary**

In a nutshell, StratML is an XML vocabulary and schema for crafting strategic plans. These components include but are not limited to corporate mission statements, policy documents, performance plans, strategic reports, organizational goals, and individual statements of purpose. From an organizational standpoint, StratML enables the sharing, indexing, referencing, discovery, reuse, and analysis of embedded elements within these plans, along with the names and descriptions of stakeholder groups. StratML promotes the concept of strategic alignment of records created by organizations in the routine course of their business processes. From a discovery viewpoint, StratML can assist organizations and individuals find potential partners that share common or complementary goals and objectives. Additionally, it can facilitate stakeholder feedback for strategic goals and objectives, while providing centralized updating and maintenance of such information. From a Federal IT ecosystem perspective, StratML can reduce time delays and data inconsistencies associated with maintaining overlapping information in stovepipe systems by automatically referencing a single authoritative source.

## The Scenario

We are not trying to overreach and say that an open, machine-readable standard could locate a terrorist and stop an bombing or attack, but StratML could be used to craft strategic agreements between entities such as the FBI and DOJ to first responders (e.g., police, firemen, EMS, etc.) to better handle “post” event matters. However, strategic agreements could also be put into place to deal with “pre-event” matters as well. In my Part One: StratML Toolkit & StratML Cloud report I present how volunteer groups could aid Federal Agencies like the EPA in the event of an oil spill. In this piece we will try to leverage the capabilities of StratML to help raise the “observation of suspicious people or suspicious packages” awareness levels to possibly help to stop an attack, reduce loss of life and, or minimize injury.

In Part One: StratML Toolkit & StratML Cloud report we look at how strategic agreements between interested parties (e.g., EPA, Coast Gard, environmental groups, etc.) that share common goals or interests could work closer together during an oil spill clean-up effort off the coast of Southern California. However, looking at the Boston Marathon attack requires not only a different set of eyes, but a stronger stomach. Case in point: Cleaning birds doused in oil with dishwashing liquid on a once pristine beach is far different than witnessing people loss multiple limbs and being killed on Boylston Street.

Not only could the FBI and DOJ put various strategic agreements in place with local law enforcement and race organizers, but also various volunteer groups that are willing to participate. This is where StratML “alignment” capabilities may be leveraged in the sharing, indexing, referencing, discovery, reuse, and analysis of embedded elements within these plans, along with the names and descriptions of stakeholder groups. It must be reiterated that StratML is not to replace technologies and protocols already in place, but is meant to augment them to create improved alignment between all parties involved.

In theory a StratML Exchange could be a place where entities participate in offering their goods and services, along with locating and exchanging ideas with interested parties, which could ultimately lead to consummating strategic agreements. For example, volunteer groups comprised of students, teachers and, or community members could be used to augment the local law enforcement. By augment I mean they can look out for and report suspicious people and, or packages to others involved in law enforcement via simple devices such as walky-talkies or any type of two-way communication offering. Accordingly, if a “bombing” or “attack” does occur agreements could also be in place with local hospitals and doctors, so the immediate medical response infrastructure is better prepared to help regarding this type of event.

The open, machine-readable technologies portrayed in this document are not cool or sexy, but saving lives and minimizing injury is very serious stuff. These are the technologies that are not mentioned in the same breath as IPO’s, but they are needed to better deal with manmade and natural catastrophic events. Looking at the aftermath videos portrays a scene of terror and suffering at an unimaginable scale. As a result, pro-active and reactive measures should be put into place to better deal with situations like what happened at the Boston Marathon on April 15, 2013. Technology will play an important part, but ultimately we must look at how the human factor comes into play.

## **The Human Factor**

Technology has been the main focus of this short piece, but what is it meant to protect? People with human emotions that have friends and family, which provide the fabric for their respected communities. This fabric can be traced to native Hopi dancers, Ansel Adams B&W prints, and Aaron Copland symphonic compositions. It is here where we find race participants, supporters, and protectors all working together to promote harmony. From the runners pushing their bodies to the limit to people handing out water bottles to folks along the race route cheering to the policemen observing the surroundings, each plays an important part in the whole. Accordingly, new technologies could be used to help promote safer environment for all.

## **Postscript**

In the StratML: Private & Public Sector Uses White Paper many areas are touched upon, which include earthquakes and hurricanes, but these are dealt with as “post” event uses of the technology. In this work the primary goal was to leverage the capabilities in a “pre” event scenario to raise the awareness factor to not only help thwart a “bombing” or “attack”, but also help to reduce loss of life and or, minimize injury if a “bombing” or “attack” does in fact take place. We also must manage expectations properly. Hence, the contents in this document are only ideas and concepts and should be looked at as such. There is nothing wrong in trying to solve problems by leveraging the use of new technologies, but overselling ideas and concepts most often leads to both a false set of expectations, along with fostering a lack of credibility. However, trying to stop an event like the 2013 Boston Marathon event from ever happening again is well worth the effort.

# References

## Part One

### **AIIM**

<http://www.aiim.org/>

### **DOJ**

<http://www.justice.gov/>

### **EPA**

<http://www.epa.gov/>

### **FBI**

<http://www.fbi.gov/>

### **GPRA**

<http://www.gpo.gov/fdsys/pkg/PLAW-111publ352/pdf/PLAW-111publ352.pdf>

### **OASIS**

<https://www.oasis-open.org/>

### **StratML**

<http://xml.fido.gov/stratml/index.htm>

### **W3C**

<http://www.w3.org/>

## Part Two

### **Breaking Gov - Episode 3 Federal IT Spending**

<http://breakinggov.com/2011/08/16/the-hard-numbers-of-government-debt-federal-spending-episode/>

### **Breaking Gov - Episode 5 Federal IT Spending**

<http://breakinggov.com/2011/09/15/an-unlikely-innovator-in-technology-adoption-federal-spending/>

### **Bulldog Drummond Education Blog One (When You Know Better, You Do Better)**

<http://bulldogdrummond.com/blog/4672#comments>

### **Bulldog Drummond Education Blog Two (Always Be Learning)**

<http://bulldogdrummond.com/blog/5225>

### **CIO Magazine**

[http://www.cio.com/article/606636/How\\_Cloud\\_Computing\\_and\\_Mobile\\_Devices\\_Are\\_Changing\\_Your\\_Application\\_Strategy#disqus\\_thread](http://www.cio.com/article/606636/How_Cloud_Computing_and_Mobile_Devices_Are_Changing_Your_Application_Strategy#disqus_thread)

**Incubating New Kinds of Collaborations with Emerging RDF/XML Technologies**  
<https://www.oasis-open.org/committees/download.php/4621/HumanMLinCollaborations.doc>

**SIA Pilot-6 Improving Rapid Emergency Response for 4th SOA eGov**  
<http://humanml.cim3.net/forum/irsc-forum/2007-09/msg00002.html>

**Federal Region 4 Semantic Interoperability Pilot Project**  
<http://137.227.242.48/region4cop102904.ppt>

**StratML: Private & Public Sector Uses by Ranjeeth K. Thunga & R. Russell Ruggiero**  
<http://xml.fido.gov/stratml/references/StratML-PrivatePublicSectorUses.pdf>

**Part One – StratML Toolkit & StratML Cloud**  
<http://xml.fido.gov/stratml/references/StratMLToolkitCloud.pdf>

# Copyright

The content contained in this self-funded report may not be used unless authorized by the author.

Date: January 27, 2014

**R. Russell Ruggiero**

Please Note: If any content in this report is used without written permission from the author (R. Russell Ruggiero) legal action will be taken by law firm retained by the author.