

# Using DNSSEC Experience To Prevent Cyber Attacks

## Overview

In December 2009, all federal government agencies that used the .gov delegation had to deploy DNS Security Extensions (DNSSEC) for their domains. DNSSEC adds a layer of security to DNS so that computers can verify that they have been directed to the proper server, preventing the most dangerous types of DNS attacks and cyberhacking.

Implementing DNSSEC is especially critical for high-risk government sites because they are often targeted by cyber attackers and are expected by users to be safe. Even though the technical community has been working on DNSSEC for two decades, cyber attacks are on the rise – a big reason why the federal government initiated such a program.

DNS is the backbone of the Internet's infrastructure and without it, web sites simply won't work. Once hackers have control over a DNS server, they have free reign to mislead and redirect users into unsafe territory. Government and other critical industries such as banking, online retail, healthcare and education are also prime candidates for DNSSEC as these industries are ripe for potential attackers.

One of those groups that had to transition was The Global Learning and Observations to Benefit the Environment (GLOBE) program, a worldwide hands-on, primary and secondary school-based science and education program. They support students, teachers and scientists who work in close partnership with NASA, NOAA and NSF Earth System Science Projects in study and research about the dynamics of Earth's environment.

Even though nearly 80% of these companies missed the DNSSEC deadline, the GLOBE transition was smooth because they used Dyn and DynECT Managed DNS.

## The Dyn Difference

GLOBE set out to find a solution that would be simple and fast. By using DynECT Managed DNS, they were able to

CLIENT DETAILS

- \* Global science & education program that works with NASA
- \* More than a decade of service
- \* More than 54,000 GLOBE-trained teachers worldwide

KEYS TO SUCCESS

- \* DNSSEC experience helped transition
- \* Ease of use with DynECT Managed DNS
- \* Increased security against potential cyber attacks

get a comprehensive managed DNS solution that comes with DNSSEC as part of its standard package. There was no additional cost for this crucial service.

As an early adopter of DNSSEC, Dyn now has years of operational DNSSEC experience to share with customers and is proud to provide a comprehensive solution and interface that allows users to enable DNSSEC by making just a few selections and clicks of the mouse.

"Dyn remains committed to making the Internet a safer place, one domain at a time," Tom Daly, Dyn President and CTO said.

## Results

"I'm glad that the DNSSEC service worked as well as it did," Mark Sallee, GLOBE Systems Administrator said. "I'm sure other .gov sites would benefit from partnership with the service provided by Dyn since the usual setup is complicated and probably many systems administrators have not yet had much experience with key creation, signing and rollover.

"We were required by NASA to migrate our .gov domain to use DNSSEC and we were fortunate that DynECT Managed DNS was an option to assist us," Sallee continued. "The transition was smooth, the customer service was responsive and the user interface made the rather complicated process quite simple."

How can Dyn help make your IaaS life easier? Email us at [sales@dyn.com](mailto:sales@dyn.com) or call us at 1.888.840.3258.

## Uptime is the Bottom Line.

Copyright © 2012 Dyn. All rights reserved. DynECT is a trademark or registered trademark of Dyn and such marks are protected by law. [001 0112 JLP]

+1 888 840 3258  
[sales@dyn.com](mailto:sales@dyn.com)  
<http://dyn.com>

150 Dow Street  
Manchester, NH  
03101 USA