THE CYBERSECURITY EXECUTIVE ORDER

orbus software

WHAT IS THE NIST CYBERSECURITY FRAMEWORK?

IN MAY 2017

President Trump signed the "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" Executive Order (EO).

It touched on a number of issues but the major take away was that, effective immediately,

federal agencies were required to start implementing The National Institute of Standards and Technology Cybersecurity Framework.

FEDERAL AGENCIES

NIST

The NIST CSF is a policy framework for computer security guidance on how organizations can assess and improve their ability to prevent, detect, and respond to cyberattacks. Let's take a look at the executive order in more detail.

FIRST SECTION

### CYBERSECURITY OF FEDERAL NETWORKS

This Section emphasizes the importance of modernizing the IT of the executive branch of the government and ensuring a level of cybersecurity that is commensurate with its importance.

To this end, it goes on mandating that all agency heads implement the NIST framework.

90

The EO also stipulates that within 90 days, agency directors must provide a report detailing the actions aimed at mitigating risk and bolstering the overall security that were taken within their organization.

Apart from this high-level report, they will need to present a detailed, agency-specific plan for the future deployment and implementation of the NIST CSF.
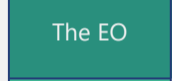
The EO borrows from the framework's language and reaffirms the need for federal agencies to prioritize shared IT services in their planning, which demonstrates the importance of the framework in building what the administration calls

"a modern, secure, and more resilient executive branch IT architecture".

SECOND SECTION

CYBERSECURITY OF CRITICAL INFRASTRUCTURE

2013

The second section reinforces a point raised in the 2013 executive order that resulted in the creation of the NIST CSF.

It deals with the importance of safeguarding critical infrastructure (i.e. that might have catastrophic effects on the health and safety of a large number of people if affected) against cyber threats.

The present EO charges the heads of agencies with:

1 Demanding feedback from these high-importance entities.

2 Identifying other authorities and mechanisms that may help to ensure a better level of cybersecurity.

3 It also asks a number of federal agencies to conduct investigations into the policies that are currently in place for promoting and protecting market transparency of cybersecurity risk management practices (specifically, as they relate to automated cyber threats, cyber-related power outages, and cybersecurity risks for military systems).

THIRD SECTION

CYBERSECURITY FOR THE NATION

Concerned with cybersecurity from the point of view of the general public and it emphasizes the need for a secure internet and a well-trained cybersecurity workforce.

90 Within 90 days, no less than eight heads of departments must produce a joint report describing America's cyber deterring capabilities.

2 Secondly, it requires the Secretaries of Homeland Security, State, Treasury, Defense, and Commerce to present reports to the President laying out their organizations' international cybersecurity priorities.

The Secretary of State will then use the findings to create a clear strategy for international cybersecurity cooperation.

SECRETARY OF STATE

The EO assigns agency leaders to analyze whether the US is investing sufficiently in the training and education of a competent future cybersecurity workforce, but also to evaluate similar development efforts conducted by allies.

LET iSERVER HELP

The renewed emphasis placed on cybersecurity means the NIST framework will become a central preoccupation for your agency.

iServer is a leading Business & IT Transformation platform that will help you quickly deploy the NIST framework and then offer you access to all the tools you'll need to manage it.

Here is why you should choose iServer:

Intuitive Microsoft Visio User Interface

Requires Minimal Training

High Configurability

Speed of Deployment

Great Presentation Tools