

Project Charter

Governor's Executive Information Security Team (GEIST)

Sponsorship

West Virginia Office of Technology (OT)
Chief Technology Officer (CTO)

Members

(As of 08/28/08)

Jim Richards, CISO - *Chairperson*

ISAs

Robert Beaver – MAPS
Debbie Browning – Commerce
Jerry Forren – DEP
Rocco Fucillo – DHHR
Donna Lipscomb – Administration (acting)
David Kovarik – PSC
Mendy McClure – DOT
Erica Mani – Department of Revenue
Tiffany Redman – Education and the Arts

Non-ISA Members

Robert Allender – Commerce
Brenda Bates – Education and the Arts
Mary Behling – Commerce
Debora Blankinship – DHHR, OIG
Bob Bryant – Commerce
Sam Butcher - Commerce
Ellen Cannon – DHHR
Rob Dixon – OT
Jim Elzey – DHHR
Ralph Goolsby – Commerce
David Kessler – Commerce
Sue Ann Lipinski – OT
Suzanne Lopez – OT
Sallie Milam – Privacy Office
Pat Miller – DHHR
Mike Morris – DHHR
Ron Nestor – DHHR
Robert Paulson – DHHR
Les Smith – Commerce
Heidi Talmage – DHHR
Darlene Thomas – DHHR
JoAnn Twohig – DOT
David Warner – Economic Development
Joyce Watson – Commerce
Jim Weathersbee – OT

Project Charter

Governor's Executive Information Security Team (GEIST)

Steering Body

Office of Information Security and Controls (OISC)

Purpose

The Governor's Executive Information Security Team (GEIST), led by the office of Information Security and Compliance, chaired by the Chief Information Security Officer (CISO), and mandated by the Governor's Executive Order 6-06, is comprised of representatives who have been appointed by Cabinet Secretaries from all Executive Branch department-level organizations, with appropriate staff support, management and leadership roles.

Mission

The mission of the GEIST is to reduce overall security related risk to State IT systems, and all data, through the application of appropriate procedures, processes, and controls, with an emphasis on administrative controls. This includes an elevated understanding of the business critical data and systems, data classification, cultural change, facilitating audits, business continuity, and user awareness of individual and collective responsibilities in the protection of information confidentiality, integrity, and availability.

Membership

GEIST membership will consist of Executive Branch agency Information Security Administrators (ISA), who have been appointed by their respective Cabinet Secretaries. ISA's may designate non-ISA members to support their effort. Membership will also include OISC representation, as appropriate. Criteria for ISA selection includes the following:

- Frequent contact with agency Cabinet Secretary
- Ability to represent agency Cabinet Secretary at GEIST meetings
- Institutional knowledge of agency
- Authority to get things done within their respective agency
- Ability to assemble ad hoc "virtual teams" for specific tasks or assignments

GEIST Members have the following responsibilities:

- Completing (or delegating) all assignments and requests
- Completing an IT-related risk analysis of agency systems, rating systems by business criticality, and documenting threats and vulnerabilities
- Overseeing the development, testing, and maintenance of business continuity and/or Continuity of Operation (COOP) plans

Project Charter

Governor's Executive Information Security Team (GEIST)

- Overseeing the classification of agency systems, as well as both electronic and non-electronic forms of data
- Overseeing the completion of mandatory information security training for all agency employees
- Assisting the OISC in its Executive Branch-wide mission to develop information security policy, to train in that policy, to audit for policy compliance, and to assure the effective remediation of findings of deficiencies or non-compliance with that policy
- Reviewing any deficient audit findings and rectifying the conditions to a satisfactory status

The GEIST may create temporary or permanent subgroups for any purpose consistent with this charter. Such subgroups take their direction from and report to the CISO.

Meetings and Communication

GEIST ISA Members must attend all meetings, or send an appropriate substitute(s). The substitute needs to be identified by name, and will act as the ISA in any consensus related discussion. Repeated absence is basis for review of the appointment. Members will meet quarterly, or as needed, at the discretion of the CISO. Members will communicate by email, teleconference, and/or by video conference, as often as needed to fulfill these responsibilities within time frames agreed upon by the GEIST.

Ongoing work and discussions will be handled via informal conferencing and email, a GEIST discussion listserv, and other media as warranted.

Guests may be invited to GEIST meetings, and should be communicated to the Chairperson, by email, at least 24 hours prior to the meeting date.

Responsibilities of CISO and the OISC

The CISO will be responsible for the following:

- Serving as chairperson and leader/facilitator for GEIST meetings
- Scheduling and organizing meetings
- Setting and prioritizing items for the agenda
- Appointing a recorder for meeting minutes
- Reviewing and distributing meeting minutes
- Being available to GEIST members for discussion on Information Security and IT-related topics of interest or concern
- Maintaining regular communication with the CTO on GEIST activities

Project Charter

Governor's Executive Information Security Team (GEIST)

- Acting as a liaison to other entities, such as the Privacy Office
- Encouraging active participation from all GEIST members

The OISC as a whole will be responsible for the following:

- Providing an appropriate audience for an ISA's Information Security concern, and, as appropriate, taking the knowledge gained from a discussion of this concern, and sharing insight with the group as a whole.
- Ensuring that the GEIST steadily pursues its mission by assisting and supporting a range of activities that are aligned with the dimensions of its purpose as set forth in the GEIST charter
- Ensuring that objectives, benchmarks, and metrics are set and used for measurement of progress
- Ensuring that the standards and processes defined in the GEIST charter are observed
- Working with subcommittee leaders to measure and encourage progress.
- Highlighting opportunities for collaboration on technology initiatives and helping to facilitate collaborative activities
- Soliciting input from all members on GEIST products (such as GEIST sponsored policies, procedures, standards, recommendations), and incorporating member input into revisions as appropriate (see Decision Making)

Decision Making

A quorum (having two-thirds of ISA membership present at the meeting) is required in order to make any changes to the GEIST charter or carry security-related recommendations upward to the Cabinet Secretaries, the Governor's Office, the CTO, or any other executive authority. GEIST members are expected to represent their respective offices, and should resist representing personal interests to that end. Members will arrive at a recommendation by following the procedure outlined below:

a) Consensus: This does not require unanimity, since members may still disagree with the final result; BUT all members do agree to support the outcome. A consensus will be reached when all members can say they agree with the decision OR have had their "say" and were unable to convince the others of their viewpoint. If a consensus cannot be reached, the GEIST chairperson will proceed to step b):

b) Voting: In taking a vote, the majority of votes will win. Members must be present to vote. If the vote is tied, the GEIST Chairperson will proceed to step c):

Project Charter

Governor's Executive Information Security Team (GEIST)

c) The chairperson will make the final recommendation. The CTO has the authority to override any recommendation.

Timeline

The GEIST was established in 2007, and will function indefinitely until such time as the Governor, or both the CTO and the GEIST chairperson (the CISO), with the Governor's approval, deem its functioning unnecessary.

GEIST members possess no term limits; however, changes in Cabinet Secretary appointment may necessitate changes in ISA selection.

Amendment to Charter

This charter is a "living document" that may be changed, modified, or otherwise amended as required to guide the GEIST. It is a controlled document and, as such, will be only be substantively modified following the decision making process specified above.