MILITARY DEPARTMENT OF INDIANA
JOINT FORCES HEADQUARTERS – INDIANA
ADJUTANT GENERAL'S OFFICE
2002 SOUTH HOLT ROAD
INDIANAPOLIS, INDIANA 46241-4839

Indiana Civilian Cyber Corps (ICCC) Standard Operating Procedure (SOP)

As of 29 July 2026

Program Mission:

The ICCC is an organization of qualified individuals dedicated to increasing cybersecurity awareness, capability and capacity throughout Indiana. The ICCC is meant to act as a catalyst for collaboration amongst Hoosier cybersecurity professionals, and is capable of providing low to no-cost training, advisement, and incident response to Hoosier organizations.

Membership:

- **Member Types:**
  - *Volunteer:*
    - ICCC Volunteers are considered experts in at least one cybersecurity domain, and have been recognized as such
      - They are individuals who are capable and willing to accomplish all aspects of the ICCC's mission, to include incident response
    - Volunteers will be requested to deploy for cyber incident response activities within the state of Indiana
      - This is annotated in IC 10-16-22 Sec. 2. (a))
    - Volunteers currently require a DoD 8140 certification
      - This requirement is a current SOP, and may change per IC 10-16-22 Sec. 2. (a)
      - Common certifications include CompTIA Security+, CISSP, CISM, GSEC, CISA, GCIH

- *Advisor:*
  - ICCC Advisors are considered knowledgeable in their respective fields, but either are unable to deploy due to a conflicting role, or they have not obtained a DoD 8140 certification
    - Advisors include members who are experts in a cyber-adjacent field (e.g., a cyber law expert) as well as individuals in the law enforcement community (who expect to respond to a cyber incident in another capacity)
  - Advisors are still able to participate in train and advise events, as well as ICCC meetings and exercises

- **Member Requirements:**
  - *Entry Requirements:*
    - Successfully pass a criminal history check
      - Required per IC 10-16-22 Sec. 2. (b))
    - Complete and sign documentation (required per current SOPs):
      - Member Application
      - Acceptable Use Policy
      - Non-Disclosure Agreement
      - Advisor/Volunteer Agreement
  - *Annual (Maintenance) Requirements:*
    - Attend one in-person event each calendar year
      - Events include meetings, exercises, training, advisement, and incident response
- **Member Applications Process:**
  - 1) Member submits completed documentation to ICCC Program Manager
  - 2) Program Manager reviews documentation and requests that the INNG Provost Marshall and the ISP each accomplish a background check on the applicant
  - 3) If the background checks are clear, then the Program Manager refers the applicant to TAG, who retains the authority to invite and appoint members to the ICCC
  - 4) If TAG accepts the member's application, then the Program Manager provides a welcome packet to the applicant, identifying them as an official member of the ICCC

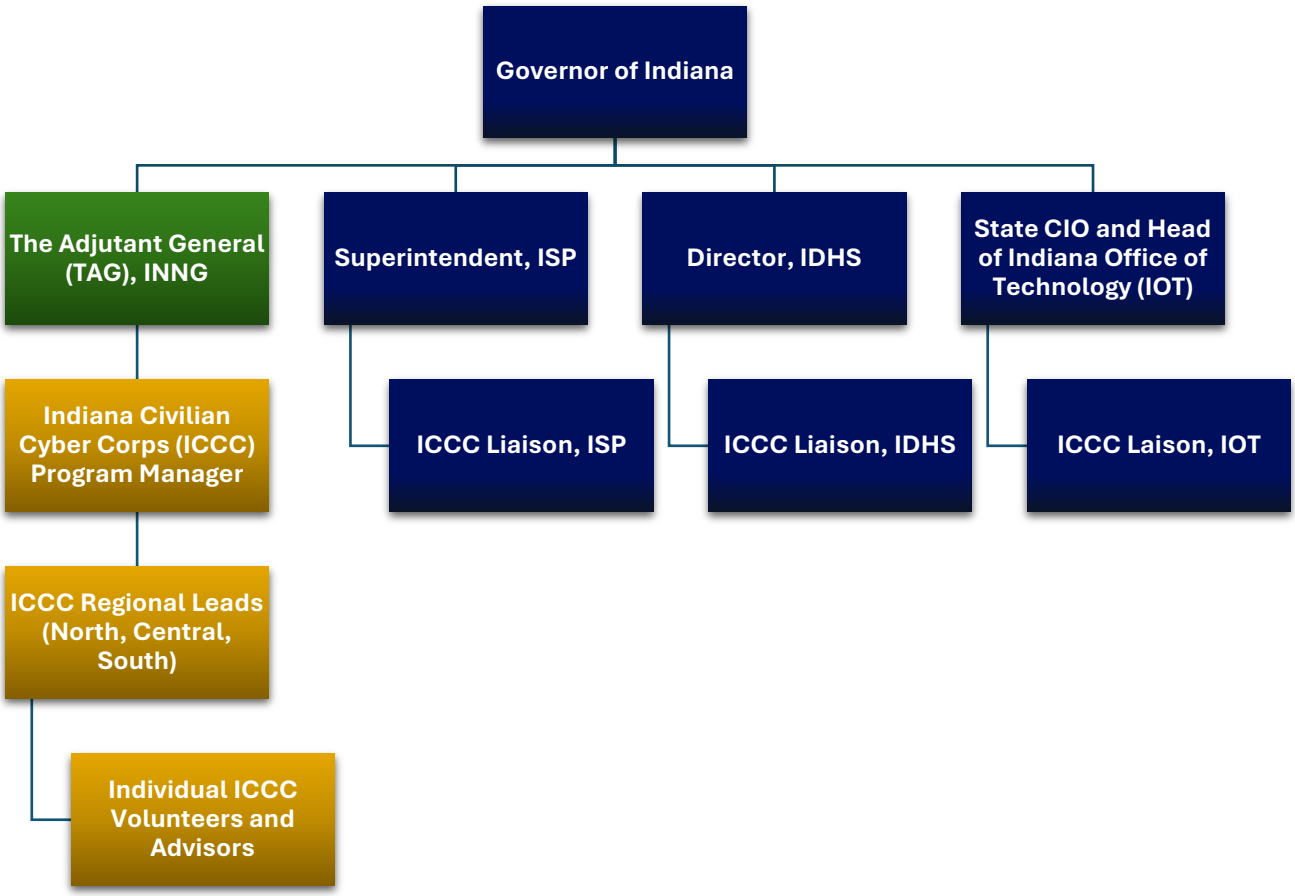
<u>Clientele</u>:

- Per IC 10-16-1-8.5, a Cybersecurity Client may include a state agency, political subdivision, state educational institution, critical infrastructure facility, or critical infrastructure utility
- **Clientele Offerings:**
  - *Training:*
    - Cybersecurity experts in the ICCC will visit the client's facility or an intermediate location to provide either a 1-hour seminar or a 3-hour course on cyber hygiene
      - Seminars and courses can be expanded, and specific topics can be requested

        - Specific topics may include (but are not limited to) threat intelligence, disaster response, risk management, and network security
    - *Advisement:*
        - ICCC cybersecurity experts will visit the client's facility or an intermediate location to provide over-the-shoulder advisement and/or face-to-face discussions on your information systems
            - Advisement may include vulnerability assessments, threat modeling, and business impact analysis
    - *Incident Response:*
        - ICCC volunteers will visit your organization to provide over-the-shoulder assistance with incident detection, response, mitigation, reporting, recovery, remediation, and lessons learned
- **Client Requirements:**
    - *Status:*
        - Per IC 10-16-1-8.5, a Cybersecurity Client must be a:
            - State agency (as defined in IC 4-1-10-2)
            - Political subdivision (as defined in IC 36-1-2-13)
            - State educational institution (as defined in IC 21-7-13-32)
            - Critical infrastructure facility (as defined in IC 35-46-10-1)
            - Critical infrastructure utility (as defined in IC 35-46-10-1)
    - *Documentation:*
        - Clients must accept ICCC training and assistance (i.e., incident response) in writing, per IC 10-16-22 Sec. 6. (d) and IC 10-16-22 Sec. 7. (d)
            - Per IC 10-16-22 Sec. 7. (d), TAG "may" enter into a full contract with the client, but technically per IC 10-16-22 Sec. 7. (c), TAG only is required to "indicate in writing" that the ICCC volunteer is authorized to provide assistance to the cybersecurity client (with a single written document able to initiate the deployment of more than one ICCC volunteer)
        - Currently, per local SOP, a "Client Agreement Professional Services Contract" is required for an organization to become a client of the ICCC
- **Client Application Process:**
    - 1) Client submits completed documentation to ICCC Program Manager
    - 2) Program Manager reviews documentation and requests that the INNG Provost Marshall and the ISP each accomplish a background check on the applicant
    - 3) If the background checks are clear, then the Program Manager refers the applicant to TAG, who retains the authority to invite and appoint members to the ICCC
    - 4) If TAG accepts the member's application, then the Program Manager provides a welcome packet to the applicant, identifying them as an official member of the ICCC

Program Management:

- The ICCC is a subdivision of the Indiana Guard Reserve (IGR) administered by the Adjutant General (TAG) of Indiana, established in Indiana Code (IC) 10-16-22 and maintained under IC 10-16-8
- **Hierarchy:**
  - Commander, ICCC (TAG)
    - Program Manager, ICCC
      - Regional Lead (North, Central, South)
        - Local Volunteer/Advisor (North, Central, South)



- **Authorities:**
  - *Commander, ICCC (TAG)*
    - Invites and appoints members to the ICCC per IC 10-16-22 Sec. 2. (a)
    - Calls for annual ICCC member meetings as well as critical incident training and exercises, per IC 10-16-22 Sec. 5.
    - Prescribes the manner that clients may request training, per IC 10-16-22 Sec. 6. (a)
    - Deploys the ICCC, per IC 10-16-22 Sec. 6. (b)
    - Accepts clients, per IC 10-16-22 Sec. 6. (c)
    - May provide training to members, per IC 10-16-22 Sec. 8. (b)
    - May provide compensation to volunteers for actual and necessary travel and subsistence expenses incurred on a deployment, per IC 10-16-22 Sec. 8. (c)
    - May establish a fee schedule for assistance, per IC 10-16-22 Sec. 8. (d)
  - *Program Manager, ICCC:*
    - Publicizes the ICCC
    - Hosts regular member meetings
    - Initiates background checks
      - Through either the INNG Provost Marshal or the Indiana State Police (ISP)
  - *Regional Leads (North, Central, South)*
    - Collects ICCC member and client applications for their region
  - *Local Volunteer*
    - Responds to cyber incidents when requested by the Commander
  - *Local Advisor*
    - Provides training and advisement to clients when requested by the Commander
- **Responsibilities:**
  - *Commander, ICCC (TAG)*
    - Maintain written documents initiating the deployment of an ICCC volunteer for either six years after the end of the deployment or the length of time required under TAG's record retention policies, per IC 10-16-22 Sec. 6. (e)
    - Publish guidelines for the operation of the ICCC, per IC 10-16-22 Sec. 8. (a)
      - Must include standards used to determine whether an individual may serve as an ICCC volunteer or advisor, and an explanation of the process by which an individual may become either an ICCC volunteer or advisor
      - Must also include an explanation of the requirements that will be imposed when a client requests and receives assistance and how the ICCC selects and prioritizes clients for assistance
  - *Program Manager, ICCC:*
    - Publicizes the ICCC to prospective members and clients
    - Identifies and manages membership and clientele
    - Manages ICCC event operations
      - Events include regular meetings and exercises, as well as training, advisement, and incident response

    - Manages the acquisition and distribution official ICCC uniforms, merchandise, and assets
  - *Regional Leads (North, Central, South)*
    - Must also be either a Volunteer or Advisor
    - Collects ICCC member and client applications for their region
    - Provides member onboarding for their region
    - Manages ICCC event logistics for their region
  - *Local Volunteer*
    - Responds to cyber incidents when requested by the Commander
    - Attends at least one in-person event each calendar year
  - *Local Advisor*
    - Provides training and advisement to clients when requested by the Commander
    - Attends at least one in-person event each calendar year
  - *Indiana Office of Technology (IOT)*
    - Shall designate a liaison to the ICCC, per IC 10-16-22 Sec. 1. (c) (1)
  - *Indiana Department of Homeland Security (IDHS)*
    - Shall designate a liaison to the ICCC, per IC 10-16-22 Sec. 1. (c) (2)
  - *Indiana State Police (ISP)*
    - Shall designate a liaison to the ICCC, per IC 10-16-22 Sec. 1. (c) (3)
    - Records client reporting of cyber incidents prior to ICCC incident response, per IC 10-16-22 Sec. 7. (a) (1)

<u>Meetings</u>:

- **Types of Meetings:**
  - *Annual Meeting:*
    - TAG calls for an annual ICCC member meeting per IC 10-16-22 Sec. 5
    - Annual meetings are expected to focus on strategic-level presentations and discussions
    - Annual meetings are expected to take place in September of each year, and should be located in an easily accessible and centralized location
      - Stout Field Building 1 or the Government Center South Conference Rooms A, B, and/or C should be utilized as primary choices for the meeting location
  - *Quarterly Meetings:*
    - Quarterly meetings are not required, but are expected to be utilized to ensure collaboration amongst Hoosier cybersecurity experts
    - Quarterly meetings are expected to focus on operational-level presentations and discussion, and may include training for ICCC members
    - Once the ICCC reaches 70 personnel per region (North, Central, and South), quarterly meetings should be held in easily accessible and centralized locations within those state regions
      - Until then, quarterly meetings should utilize similar locations to the Annual Meeting

- **Meeting Procedures:**
  - 1) TAG (for an annual meeting) or the ICCC Program Manager (for quarterly meetings) calls for an ICCC meeting, identifying the date and purpose
  - 2) The Program Manager reserves an appropriate location for the meeting
  - 3) The Program Manager requests presentation and/or discussion topics from Regional Leads and/or clients
  - 4) The Program Manager distributes meeting invitations to members
  - 5) The Program Manager (or Regional Lead for quarterly meetings) hosts the meeting, recording any attendees and significant events
  - 6) The Program Manager (or Regional Lead for quarterly meetings) provides an After-Action Report (AAR) to TAG

Exercises:

- **Types of Exercises:**
  - *Annual Exercise:*
    - TAG may call for an exercise, per IC 10-16-22 Sec. 5 (2)
    - As a default the primary annual exercise is expected to be Hoosier Cyber Defender, managed by the INNG's 127th Cyber Protection Battalion (CPB)
  - *Additional Exercises:*
    - The ICCC may host additional exercises beyond INNG-hosted events, based on growth of the organization and client and member needs
- **Exercise Procedures:**
  - 1) The lead organization's representative (either the 127th CPB or the ICCC Program Manager) calls for and hosts an Exercise Concept Development Conference (CDC), which ICCC Regional Leads are expected to participate in
  - 2) The lead organization hosts an Initial Planning Conference (IPC), which ICCC Regional Leads are expected to participate in
  - 3) The lead organization hosts a Mid-Planning Conference (MPC), which ICCC Regional Leads are expected to participate in
  - 4) The lead organization hosts a Final Planning Conference (FPC), which ICCC Regional Leads are expected to participate in
  - 5) The lead organization hosts the exercise (tabletop or full-scale), which ICCC Volunteers are expected to participate in

Training Events:

- **Types of Training Events:**
  - *Seminar (strategic/operational subjects):*
    - A minimum of two ICCC volunteers and/or advisors provide a seminar to a client's staff

    - Seminars may range wildly in subject, but are expected to be light in technical explanation and instead focus on an operational or strategic point of view
    - As a default, seminars are expected to last 1-hour, but can be expanded upon request
    - A seminar audience should contain at least 10 individuals, but has no required upper limit
  - *Course (technical subjects):*
    - A minimum of two ICCC volunteers and/or advisors provide a course for a client's staff
    - Courses are expected to delve into technical specifics in a subject, and may require attendees to have specific hardware and/or software
    - As a default, courses are expected to last 3 hours (avoiding the lunch hour), but can be expanded upon request
    - A course should contain between 5 and 30 individuals, and may combine clientele organizations if needed
- **Training Event Procedures:**
  - 1) The client may request that the ICCC provide cybersecurity training, per IC 10-16-22 Sec. 6. (a)
    - TAG's chosen representative (as a default, either the ICCC Program Manager or the INNG Joint Operations Center) may receive the client request and direct it to TAG
  - 2) TAG (or a delegated representative annotated in writing) may initiate the deployment of one or more ICCC volunteers to provide training, indicating in writing that the ICCC volunteer is authorized to provide training to the client, per IC 10-16-22 Sec. 6. (c)
    - TAG (or a delegated representative annotated in writing) should also decide at this time whether to provide compensation for actual and necessary travel and subsistence expenses incurred by an ICCC volunteer
  - 3) The document indicating authorization for training should be preserved for either six years after the end of the deployment, or the length of time required under TAG's record retention policies, whichever is longer, per IC 10-16-22 Sec. 6. (e)
    - Documentation may be preserved by the Program Manager for TAG
  - 4) The Program Manager may select individual members to present training, or may allow the Regional Lead to select members
    - A minimum of two members should be selected, with an additional member added to the deployment for every additional 50 audience members present over the first 50
  - 5) The Program Manager or Regional Lead will contact the individual members, requesting them to provide training to the client
    - Members should be informed upfront whether they will be compensated for actual and necessary travel and subsistence expenses
    - If an individual member declines, there are no repercussions, though the Program Manager or Regional Lead should annotate the declination and then move to the next member identified, until the appropriate amount of members has been selected to provide the training event
  - 6) Members arrive on-site to provide training to the client

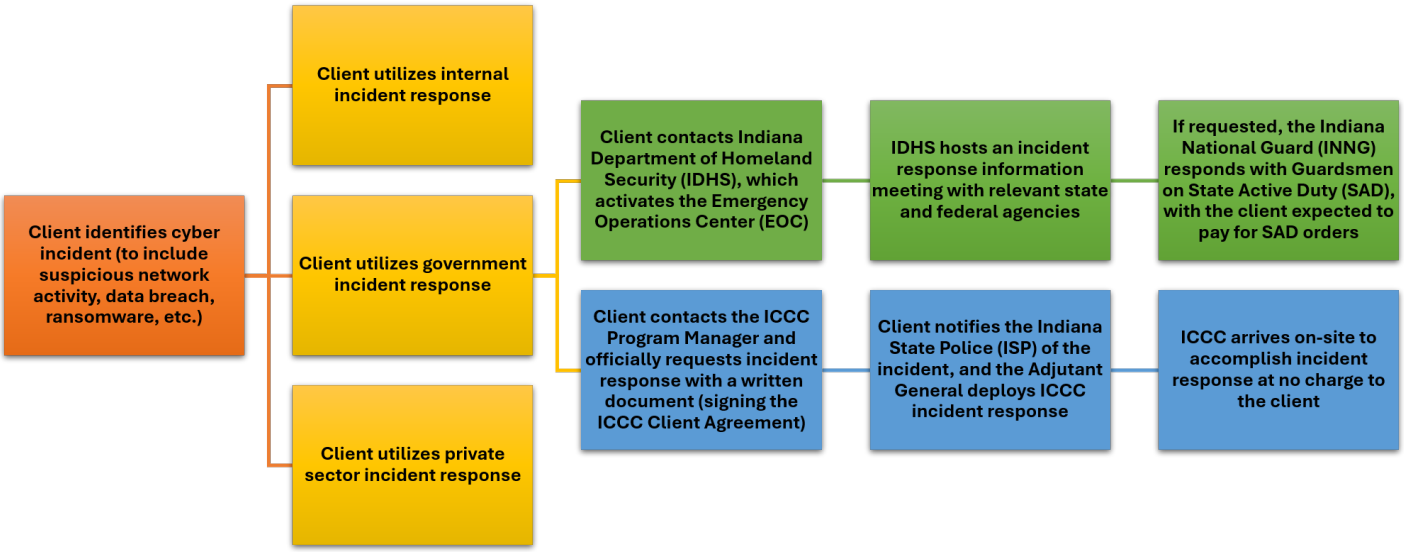
- 7) Upon completion of training, an After-Action Report (AAR) should be submitted by the lead member to the ICCC Program Manager
  - All reports should be retained for six years after the end of the deployment

Advisement Events:

- **Types of Advisement Events:**
  - *Face-to-Face (strategic/operational subjects):*
    - A minimum of two ICCC volunteers and/or advisors discuss the current state of the client's cybersecurity program, providing operational and/or strategic direction
    - Face-to-face events often include discussions on a client's budget, cybersecurity leadership investment, policies, and procedures
    - Face-to-face events may include risk management and threat modeling
  - *Over-the-Shoulder:*
    - A minimum of two ICCC volunteers and/or advisors review a client's software and/or hardware
    - Over-the-shoulder events often include discussions regarding a client's Configuration Management, Network Intrusion Protection Systems, Security Information and Event Management (SIEMS) systems, and individual logs
    - Over-the-shoulder events may include vulnerability assessments and information systems auditing
- **Advisement Event Procedures:**
  - 1) The client may request that the ICCC provide cybersecurity advisement, per IC 10-16-22 Sec. 6. (a)
    - TAG's chosen representative (as a default, either the ICCC Program Manager or the INNG Joint Operations Center) may receive the client request and direct it to TAG
  - 2) TAG (or a delegated representative annotated in writing) may initiate the deployment of one or more ICCC members to provide advisement, indicating in writing that the ICCC member is authorized to provide training to the client, per IC 10-16-22 Sec. 6. (c)
    - TAG should also decide at this time whether to provide compensation for actual and necessary travel and subsistence expenses incurred by an ICCC member
  - 3) The document indicating authorization for advisement should be preserved for either six years after the end of the deployment, or the length of time required under TAG's record retention policies, whichever is longer, per IC 10-16-22 Sec. 6. (e)
    - Documentation may be preserved by the Program Manager for TAG
  - 4) The Program Manager may select individual members to present advisement, or may allow the Regional Lead to select members
    - A minimum of two members should be selected, with an additional member added to the deployment for every additional topic of advisement the client has requested beyond the first two

- 5) The Program Manager or Regional Lead will contact the individual members, requesting them to provide advisement to the client
  - Members should be informed upfront whether they will be compensated for actual and necessary travel and subsistence expenses
  - If an individual member declines, there are no repercussions, though the Program Manager or Regional Lead should annotate the declination and then move to the next member identified, until the appropriate amount of members has been selected to provide the advisement event
- 6) Members arrive on-site to provide advisement to the client
- 7) Upon completion of advisement, an After-Action Report (AAR) should be submitted by the lead member to the ICCC Program Manager
  - All reports should be retained for six years after the end of the deployment

<u>Incident Response Process</u>:



<u>Incident Response</u>:

- **Types of Incident Response:**
  - *Over-the-Shoulder:*
    - A minimum of two ICCC Volunteers provide guidance on incident response by working with a client IT or cybersecurity representative and reviewing the client's information systems, accounts, logs, and physical systems
    - Volunteers will not physically interact with any client systems
    - Volunteers will not connect to any client systems virtually or physically
    - Over-the-shoulder is the default rapid response posture

- *Hands-on-Keyboard:*
  - A minimum of two ICCC Volunteers provide full Digital-Forensics Incident Response (DFIR)
  - Volunteers may physically interact with client systems that have been approved in writing by the client and TAG
  - Volunteers may connect to client systems virtually or physically that have been approved in writing by the client and TAG
  - Volunteers will NOT provide hands-on-keyboard without these activities being approved in writing

- **Incident Response Process:**
  - 1) The cybersecurity client shall notify ISP upon the occurrence of a cybersecurity incident before requesting response capabilities of the ICCC, per IC 10-16-22 Sec. 7. (a)
  - 2) The client may request TAG to deploy one or more ICCC volunteers to provide rapid response assistance, per IC 10-16-22 Sec. 7. (b)
    - TAG's chosen representative (as a default, either the ICCC Program Manager or the INNG Joint Operations Center) may receive the client request and direct it to TAG
  - 3) TAG may initiate the deployment of one or more ICCC volunteers, indicating in writing that the ICCC volunteer is authorized to provide assistance to the client, per IC 10-16-22 Sec. 7. (c)
    - TAG should also decide at this time whether to provide compensation for actual and necessary travel and subsistence expenses incurred by an ICCC volunteer
  - 4) The document indicating authorization for deployment should be preserved for either six years after the end of the deployment, or the length of time required under TAG's record retention policies, whichever is longer, per IC 10-16-22 Sec. 7. (f)
    - Documentation may be preserved by the Program Manager for TAG
  - 5) The Program Manager may select individual volunteers to deploy, or may allow the Regional Lead to select volunteers
    - A minimum of two volunteers should be selected, with an additional volunteer added to the deployment for every additional 30 networked devices present on the client's network over the first 30
  - 6) The Program Manager or Regional Lead will contact the individual volunteers, requesting their deployment to provide rapid response assistance to the client
    - Volunteers should be informed upfront whether they will be compensated for actual and necessary travel and subsistence expenses
    - If an individual volunteer declines, there are no repercussions, though the Program Manager or Regional Lead should annotate the declination and then move to the next volunteer identified, until the appropriate amount of volunteers has been deployed
  - 7) Volunteers arrive on-site to provide rapid response assistance to the client
    - Assistance may include, but is not limited to, Detection, Response, Mitigation, Reporting, Recovery, Remediation, and Lessons Learned activities

    - As a default, assistance is expected to last for 48 hours, with any extension annotated in writing
    - Volunteers should annotate incident response activities in a journal, marking the exact times each event occurs
  - 8) Volunteers should provide updates every two hours to the Program Manager
    - If the incident is beyond the level of expertise for the volunteer(s) involved, the Program Manager should be informed
    - If the incident is beyond the level of expertise (or scope) of the ICCC, then the client should be advised to utilize additional incident response forces (as a default, the 127th Cyber Battalion will be recommended)
  - 9) If additional assistance is required beyond 48 hours, the client must request an extension of assistance
  - 10) Upon completion of rapid response, an After-Action Report (AAR) should be submitted by the lead volunteer to the ICCC Program Manager, including all journalled incident response activities
    - All reports should be retained for six years after the end of the deployment

<u>Legal Protections and Documentation Language</u>:

- **Protections in Indiana Code (IC):**
  - IC 10-16-22 Sec. 3. (a): A civilian cyber corps volunteer or civilian cyber corps adviser is not an agent, employee, or independent contractor of the state of Indiana for any purpose and has no authority to bind the state of Indiana with regard to third parties.
  - IC 10-16-22 Sec. 3. (b): The state of Indiana is not liable to a civilian cyber corps volunteer or civilian cyber corps adviser for personal injury or property damage suffered by the civilian cyber corps volunteer or civilian cyber corps adviser through participation in the civilian cyber corps.
  - IC 10-16-22 Sec. 4. (a): The adjutant general, the military department, and the state of Indiana are immune from tort liability for acts or omissions by a civilian cyber corps volunteer or civilian cyber corps adviser as provided in this chapter.
  - IC 10-16-22 Sec. 4. (b): A civilian cyber corps volunteer or civilian cyber corps adviser is subject to the same civil and criminal immunity protections as a member of the Indiana National Guard under IC 10-16-7-7(b) and IC 10-16-7-7(d) for any act done by the civilian cyber corps volunteer or civilian cyber corps adviser in the discharge of the civilian cyber corps volunteer's or civilian cyber corps adviser's official duty under this chapter.
  - IC 10-16-22 Sec. 9. (a): Information that is voluntarily given to the civilian cyber corps or obtained under this chapter that would identify or provide as a means of identifying a person or cybersecurity client, and the disclosure of which may: (1) cause the person or cybersecurity client to become a victim of a cybersecurity incident; or (2) disclose a person's or cybersecurity client's cybersecurity plans or cybersecurity related practices,

procedures, methods, results, organizational information system infrastructure, hardware, or software; is confidential and exempt from disclosure under IC 5-14-3-4.

- IC 10-16-22 Sec. 9. (b): The work product of a civilian cyber corps volunteer or civilian cyber corps adviser under this chapter is confidential and exempt from disclosure under IC 5-14-3-4.
- IC 34-13-3-3 Sec. 3. (a): A governmental entity or an employee acting within the scope of the employee's employment is not liable if a loss results from the following:
  - (1) The natural condition of unimproved property.
  - (2) The condition of a reservoir, dam, canal, conduit, drain, or similar structure when used by a person for a purpose that is not foreseeable.
  - (3) The temporary condition of a public thoroughfare or extreme sport area that results from weather.
  - (4) The condition of an unpaved road, trail, or footpath, the purpose of which is to provide access to a recreation or scenic area.
  - (5) The design, construction, control, operation, or normal condition of an extreme sport area, if all entrances to the extreme sport area are marked with:
    - (A) a set of rules governing the use of the extreme sport area;
    - (B) a warning concerning the hazards and dangers associated with the use of the extreme sport area; and
  - (C) a statement that the extreme sport area may be used only by persons operating extreme sport equipment.
  - This subdivision shall not be construed to relieve a governmental entity from liability for the continuing duty to maintain extreme sports areas in a reasonably safe condition.
  - (6) The initiation of a judicial or an administrative proceeding.
  - (7) The performance of a discretionary function; however, the provision of medical or optical care as provided in IC 34-6-2.1-54 shall be considered as a ministerial act.
  - (8) The adoption and enforcement of or failure to adopt or enforce:
    - (A) a law (including rules and regulations); or
    - (B) in the case of a public school or charter school, a policy; unless the act of enforcement constitutes false arrest or false imprisonment.
  - (9) An act or omission performed in good faith and without malice under the apparent authority of a statute which is invalid if the employee would not have been liable had the statute been valid.
  - (10) The act or omission of anyone other than the governmental entity or the governmental entity's employee.
  - (11) The issuance, denial, suspension, or revocation of, or failure or refusal to issue, deny, suspend, or revoke any permit, license, certificate, approval, order, or similar authorization, where the authority is discretionary under the law.
  - (12) Failure to make an inspection, or making an inadequate or negligent inspection, of any property, other than the property of a governmental entity, to determine whether the property complied with or violates any law or contains a hazard to health or safety.

- (13) Entry upon any property where the entry is expressly or impliedly authorized by law.
- (14) Misrepresentation if unintentional.
- (15) Theft by another person of money in the employee's official custody, unless the loss was sustained because of the employee's own negligent or wrongful act or omission.
- (16) Injury to the property of a person under the jurisdiction and control of the department of correction if the person has not exhausted the administrative remedies and procedures provided by section 7 of this chapter.
- (17) Injury to the person or property of a person under supervision of a governmental entity and who is:
  - (A) on probation;
  - (B) assigned to an alcohol and drug services program under IC 12-23, a minimum security release program under IC 11-10-8, a pretrial conditional release program under IC 35-33-8, or a community corrections program under IC 11-12; or
  - (C) subject to a court order requiring the person to be escorted by a county police officer while on or in a government building (as defined in IC 36-9-13-3) owned by a county building authority under IC 36-9-13, unless the injury is the result of an act or omission amounting to:
    - (i) gross negligence;
    - (ii) willful or wanton misconduct; or
    - (iii) intentional misconduct.
- (18) Design of a highway (as defined in IC 9-13-2-73), toll road project (as defined in IC 8-15-2-4(4)), tollway (as defined in IC 8-15-3-7), or project (as defined in IC 8-15.7-2-14) if the claimed loss occurs at least twenty (20) years after the public highway, toll road project, tollway, or project was designed or substantially redesigned; except that this subdivision shall not be construed to relieve a responsible governmental entity from the continuing duty to provide and maintain public highways in a reasonably safe condition.
- (19) Development, adoption, implementation, operation, maintenance, or use of an enhanced emergency communication system.
- (20) Injury to a student or a student's property by an employee of a school corporation if the employee is acting reasonably under a:
  - (A) discipline policy adopted under IC 20-33-8-12; or
  - (B) restraint and seclusion plan adopted under IC 20-20-40-14.
- (21) An act or omission performed in good faith under the apparent authority of a court order described in IC 35-46-1-15.1 or IC 35-46-1-15.3 that is invalid, including an arrest or imprisonment related to the enforcement of the court order, if the governmental entity or employee would not have been liable had the court order been valid.
- (22) An act taken to investigate or remediate hazardous substances, petroleum, or other pollutants associated with a brownfield (as defined in IC 13-11-2-19.3) unless:
  - (A) the loss is a result of reckless conduct; or
- (B) the governmental entity was responsible for the initial placement of the hazardous substances, petroleum, or other pollutants on the brownfield.

    - (23) The operation of an off-road vehicle (as defined in IC 14-8-2-185) by a nongovernmental employee, or by a governmental employee not acting within the scope of the employment of the employee, on a public highway in a county road system outside the corporate limits of a city or town, unless the loss is the result of an act or omission amounting to:
        - (A) gross negligence;
        - (B) willful or wanton misconduct; or
        - (C) intentional misconduct.
    - This subdivision shall not be construed to relieve a governmental entity from liability for the continuing duty to maintain highways in a reasonably safe condition for the operation of motor vehicles licensed by the bureau of motor vehicles for operation on public highways.
    - (24) Any act or omission rendered in connection with a request, investigation, assessment, or opinion provided under IC 36-9-28.7.
    - (25) Any act or omission rendered in connection with an Indiana civilian cyber corps program deployment as provided under IC 10-16-22.
- **Nondisclosure Agreement (NDA):**
    - "The information" that members are granted access to in order to perform official duties includes, but is not limited to:
        - Details pertaining to personnel (staff, contractors, volunteers, visitors, and vendors),
        - Details pertaining to ICCC and INNG operations, finances, contracts, community outreach, and official coordination or liaison,
        - Details pertaining to restricted and sensitive computer systems and networks,
        - Details pertaining to ongoing inner-office activities and matters,
        - Details pertaining to ongoing and future ICCC and INNG operations,
        - Various official and personal records or documents
    - A failure to abide by the NDA may result in:
        - Initiation of civil actions or penalties up to and including initiation of an investigation, or referral of criminal charges under the Uniform Code of Military Justice (UCMJ), per Indiana Code 10-16-6-10.
    - All members must agree to the following in writing:
        - The information may contain personally identifiable, individual and business tax and financial, medical, and law enforcement sensitive information. Such information is normally subject to security in accordance with a specific law, executive order, department order, or local policy. When handling such information, I assume the responsibility to request additional guidance from my supervisor prior to taking custody or accessing the information.
        - The information must be safeguarded at all times, in all forms, and on all devices or systems. I am not allowed to mail, electronically forward or send the information to any personal e-mail account or device.

- The information belongs to a governmental (Federal, State, Local, and Tribal) or client organization (non- governmental organization, a business, an individual, or combination thereof).
- The information presented, discussed, reviewed, stored, and created for an operation, investigation, training, and all other associated information is State of Indiana or INNG property.
- I must safeguard all information in a manner that ensures only authorized persons have access to said information. I will not disclose information to anyone not specifically authorized by the Indiana National Guard, an executive agency of the State of Indiana, or my supervisor without the direct approval of the same.
- I will return any and all ICCC, State owned, or client owned information I have in my custody or care upon release or separation from the ICCC.
- I will not share, seek, or attempt to gain access to sensitive information after my departure including information about the status of prior work cases or projects in which I was previously allowed access.
- I will immediately inform my leadership of any attempt by any unauthorized person to gain access to the information

- **Acceptable Use Policy (AUP):**
  - The AUP applies to all personnel granted access to ICCC and/or ICCC-related IT resources.
    - Unauthorized access or use of information systems is strictly prohibited and closely monitored. Usage is governed by and subject to United States and Indiana laws and policies. There is no expectation of privacy with respect to material placed on or viewed by the system with exception to specific status or statutes. In accordance with Federal and State laws, monitoring may result in acquisition, recording, and analysis of any and all data communicated, transmitted, processed or stored on the system. Anyone using ICCC-related IT resources including any devices attached to this system consents to the items listed above, but not limited to, and does so in accordance and with the understanding of being subject to administrative action, civil and criminal penalties.
  - A failure to abide by the AUP may result in:
    - Initiation of civil actions or penalties up to and including initiation of an investigation, or referral of criminal charges under the Uniform Code of Military Justice (UCMJ), per Indiana Code 10-16-6-10.
  - All members must agree to the following in writing:
    - ICCC IT resources are provided for ICCC-related activity and are to be used in a manner consistent with State of Indiana policies, regulations, and procedures, including ICCC/State of Indiana professional standards of ethical behavior.
    - Users have no right to privacy related to their use of IT Resources. Any information created or stored on IT Resources is subject to public disclosure. The State reserves the right to monitor all use of IT Resources, including email, Internet history, and Internet traffic.

- Users must protect IT Resources from unauthorized access, theft, damage, and modification. The user must lock any State-managed device when not in use and protect State provided equipment from theft and unauthorized use when outside the office.
- Users must protect all State-owned data and will not access or disclose information for which they have no authorization or business need.
- The viewing, storing, or accessing of illegal content is not permitted.
- ICCC Members will not use ICCC and/or ICCC-related IT resources to view, store, or access obscene materials, such as pornography, except when clearly required to do so in the course of their work such as may occur as part of an incident response.
- ICCC Members will may not use ICCC and/or ICCC-related IT resources to support or oppose a candidate for public office or a ballot measure in a manner contrary to Indiana laws governing the political activities of public employees.
- Use of ICCC IT resources, including the posting of information on ICCC-related environments, must comply with applicable copyright laws. When posting or downloading information to or from the internet, the user is responsible for ensuring that copyright law is not violated.
- All software installed, stored, or operated on ICCC and/or ICCC-related systems must be properly licensed, whether used for educational, professional, or private use.
- Users are not authorized to access, use, copy, modify or delete data, or grant access to others, in a manner inconsistent with ICCC and State of Indiana information security policy.
- Users may not gain access to any files, data, or systems through the use of another user's User ID and/or Password unless authorized to do so as part of an authorized operation or activity approved by an authorized individual.
- Users must not share login IDs or passwords to IT Resources with other people.
- Users may not forge or misrepresent their identity, or enable others to falsify an identity, when using ICCC and/or ICCC-related IT resources unless authorized to do so as part of an authorized operation or activity approved by an authorized individual. This type of forgery can result in criminal penalties and disciplinary action.
- Users of ICCC and/or ICCC-related IT resources with access to personally identifiable information (PII) are responsible for the continued protection and integrity of such data.
- Users are required to return IT Resources that have been provided to them by the State--computers, mobile phones, and all other devices--no later than at the time of their separation. Failure to return IT Resources will be viewed as theft and addressed accordingly.
- Users must report known or suspected violations of this agreement to their supervisor.

- **Member Agreement:**
  - Members must agree to and acknowledge the following in writing:
    - Terms of service:

- The Member understands that they are entering into the Indiana Guard Reserve as a civilian member as set forth in IC 10-16-22. The Member understands and acknowledges joining by appointment to the ICCC.

- Public Trust:
  - The Member understands and acknowledges that this appointment confers significant public trust and requires the member to always comport one's self as to not bring discredit to yourself or the organization; conduct official duties with a high degree of professionalism, and do not act officiously or permit personal feelings, prejudices, political beliefs, aspirations, animosities or friendships to influence official actions or decisions.
- The Member understands and acknowledges that the adjutant general shall establish and publish those standards of experience, education, and conduct expected of the member to maintain their appointment to the ICCC, and that those publishes standards, and this Agreement, shall compel the member to comply with all lawful direction (orders, directives, and regulations) from those appointed over the member. Failure to adhere to these standards and/or follow those orders, directives, or regulations lawfully given may constitute grounds for dismissal from the ICCC.
- Confidentiality:
  - The Member understands and acknowledges that during the course of the member's member service with the ICCC, he or she may have access to and learn about confidential, restricted, secret and proprietary documents, materials, data and other information, in tangible and intangible form, of and relating to the State, its residents and ICCC Client(s)("Confidential Information").
  - The Member understands that Confidential Information also includes other information that is marked or otherwise identified as confidential, restricted or proprietary, or that would otherwise appear to a reasonable person to be confidential, restricted or proprietary in the context and circumstances in which the information is known or used.
  - The Member further understands and acknowledges that this Confidential Information and the State's ability to reserve it for the exclusive knowledge and use of the State is of great importance and value to the State, and that improper use or disclosure of the Confidential Information by the Member will cause irreparable harm to the State, for which remedies at law will not be adequate and may also cause the State to incur financial costs, liability under confidentiality agreements with third parties, and civil damages.
  - The Member understands and agrees that Confidential Information developed by him/her in the course of the member's his/her service with the ICCC shall be subject to the terms and conditions of this Agreement as if the State furnished the same Confidential Information to the Member in the first instance. Confidential Information shall not include information that is generally available to and known by the public,

provided that such disclosure to the public is through no direct or indirect fault of the Member or person(s) acting on the Member's behalf.

- Confidentiality and Disclosure and Use Restrictions. The Member agrees and covenants:
  - to treat all marked and unmarked Confidential Information as strictly confidential;
  - not to directly or indirectly disclose, publish, communicate or make available Confidential Information, or allow it to be disclosed, published, communicated or made available, in whole or part, to any entity or person whatsoever (including other members of the ICCC) not having a need to know and authority to know and use the Confidential Information in connection with the operation of the ICCC; and
  - not to access or use any Confidential Information, and not to copy any documents, records, files, media or other resources containing any Confidential Information, or remove any such documents, records, files, media or other resources from the premises or control of the State, except as required in the performance of the Member's authorized member duties to the ICCC or with the prior consent of an authorized officer acting on behalf of the State in each instance (and then, such disclosure shall be made only within the limits and to the extent of such duties or consent).
- Nothing in this Agreement shall be construed to prevent disclosure of Confidential Information as may be required by applicable law or regulation, or pursuant to the valid order of a court of competent jurisdiction or an authorized government agency, provided that the disclosure does not exceed the extent of disclosure required by such law, regulation or order. The Member shall provide written notice of any such order to an authorized officer of the State within two (2) days of receiving such order, but in any event sufficiently in advance of making any disclosure to permit the State to contest the order or seek confidentiality protections, as determined in the State's sole discretion.
- Duration of Confidentiality Obligations. The Member understands and acknowledges that the member’s obligations under this Agreement with regard to any particular Confidential Information shall commence immediately upon the Member first having access to such Confidential Information (whether before or after the member begins member service with the ICCC) and shall continue during and after the member’s member service with the ICCC until such time as such Confidential Information has become public knowledge other than as a result of the Member's breach of this Agreement or breach by those acting in concert with the Member or on the Member's behalf.

- Security:
  - Security and Access. The Member agrees and covenants;
    - to comply with all State security policies and procedures as in force from time to time including without limitation those regarding computer equipment, telephone systems, voicemail systems, facilities access, monitoring, key cards, access

codes, State intranet, internet, social media and instant messaging systems, computer systems, e-mail systems, computer networks, document storage systems, software, data security, encryption, firewalls, passwords and any and all other State facilities, IT resources and communication technologies ("Facilities and Information Technology Resources");
  - not to access or use any Facilities and Information Technology Resources except as authorized by the State; and
  - not to access or use any Facilities and Information Technology Resources in any manner after the termination of the Member's service with the ICCC, whether termination is voluntary or involuntary. The Member agrees to notify the State promptly in the event he or she learns of any violation of the foregoing by others, or of any other misappropriation or unauthorized access, use, reproduction or reverse engineering of, or tampering with any Facilities and Information Technology Resources or other State property or materials by others.
- Exit Obligations – Upon:
  - voluntary or involuntary termination of the Member's service with the ICCC or
  - the State's request at any time during the Member's service with the ICCC, the Member shall
    - provide or return to the State any and all State property, including key cards, access cards, identification cards, security devices, network access devices, computers, other removable information storage devices, and all State documents and materials belonging to the State and stored in any fashion, including but not limited to those that constitute or contain any Confidential Information, that are in the possession or control of the Member, whether they were provided to the Member by the State or created by the Member in connection with the member's member service with the ICCC; and
    - delete or destroy all copies of any such documents and materials not returned to the State that remain in the Member's possession or control, including those stored on any non-State devices, networks, storage locations and media in the Member's possession or control.
- Self-Disclosure:
  - The member understands that immediate reporting is required for any arrested or criminal charges by civilian authorities, the term arrest includes an arrest or detention, and the term charged includes the filing of criminal charges. Furthermore, it is understood that disclosure of arrest/criminal charges is not an admission of guilt and may not be used as such, nor is it intended to elicit an admission from the member self-reporting.
- By signing, the Member acknowledges the Member's responsibility to provide information regarding any arrest and criminal charges by civilian authorities to Commander of the Indiana Guard Reserve or his/her designee and to the senior full-time ICCC administrator.

- Background Screening:
  - The Member is required to undergo a successful background screening prior to membership in the ICCC. By signing, the Member hereby consents to a background screening considered appropriate by the State. Further, the Member consents that the State may conduct periodic additional background checks at any time during the Member's service.

- Conflict of Interest:
  - The Member shall make every effort to avoid any conflict between their own personal, company or firm interests and the interests of the State or the ICCC Client(s), in all actions taken by them on behalf of the State. A Member shall abstain from duty with the ICCC when such service could cause the Member to benefit personally or cause the Members' company, firm or full-time employer to benefit from the outcome of such service. The Member will disclose any potential conflict of interest to the State. The disclosure of any potential conflict should be in writing and should describe the facts and circumstances relative to the potential conflict of interest. It will be the decision of the State as to a resolution of the conflict, if a resolution is deemed necessary. Any Member who is aware of a conflict of interest on the member's part and fails to report such shall be subject to removal from the ICCC.
- Expertise Attestation (Not applicable for non-technical mentors, leaders, and support personnel):
  - The Member attests that he or she meets any standard of expertise that may be established by the State in order to qualify as a member of the ICCC.
  - The standard of expertise for an Advisor currently includes but is not limited to having at least 2-4 years of direct involvement with cyber law, network administration, computer science, information security, security operations, incident response, and/or digital or network forensics.
  - The standard of expertise for a Volunteer currently includes but is not limited to having at least 1 Department of Defense (DoD) 8140 Cyber Workforce Certification from the DoD 8140 Qualification Matrix, and at least 2-4 years of direct involvement with information security, preferably security operations, incident response, and/or digital or network forensics that requires work role certification in that role.
- Publicity:
  - The Member hereby consents to any and all uses and displays, by the State and its agents, of the Member's name, voice, likeness, image, appearance and biographical information in, on or in connection with any pictures, photographs, audio and video recordings, digital images, websites, television programs and advertising, other advertising, sales and marketing brochures, books, magazines, other publications, CDs, DVDs, tapes and all other printed and electronic forms and media throughout the world, at any time during the period of the member's member service with the ICCC, for all legitimate business purposes of the State ("Permitted Uses"). Member hereby forever releases the State and its directors, officers, members and agents

from any and all claims, actions, damages, losses, costs, expenses and liability of any kind, arising under any legal or equitable theory whatsoever at any time during or after the period of the member's member service with the ICCC, in connection with any Permitted Use.

- Miscellaneous.
  - Pay:
    - Notwithstanding any other provision of law, ICCC members operate in a voluntary status and are not entitled to any financial compensation in exchange for the voluntary services provided, excluding allowable per diem and/or applicable travel reimbursement.
- Liability:
  - Pursuant to IC 10-16-22-4(b), a member of the ICCC is subject to the same civil and criminal immunity protections as a member of the Indiana National Guard under IC 10-16-7-7(b) and IC 10-16-7-7(d) for any act done by the ICCC member in the discharge of their official duties.
- Pursuant to IC 10-16-22-3(a), an ICCC member is not an employee, agent, or independent contractor of the state of Indiana for any purpose and has no authority to bind the state of Indiana with regard to third parties.
- The Member acknowledges that he or she may not operate automotive or other State-owned equipment without specific written authorization of the State.
- Waiver:
  - Failure to enforce any provision of this Agreement will not constitute a waiver.
- Remedies:
  - The Member acknowledges that the State's Confidential Information and the State's ability to reserve it for the exclusive knowledge and use of the State is of great importance to the State, and that improper use or disclosure of the Confidential Information by the Member will cause irreparable harm to the State, for which remedies at law will not be adequate. In the event of a breach or threatened breach by the Member of any of the provisions of this Agreement, the Member hereby consents and agrees that the State shall be entitled to seek, in addition to other available remedies, a temporary or permanent injunction or other equitable relief against such breach or threatened breach from any court of competent jurisdiction, without the necessity of showing any actual damages or that monetary damages would not afford an adequate remedy, and without the necessity of posting any bond or other security. The aforementioned equitable relief shall be in addition to, not in lieu of, legal remedies, monetary damages or other available forms of relief.