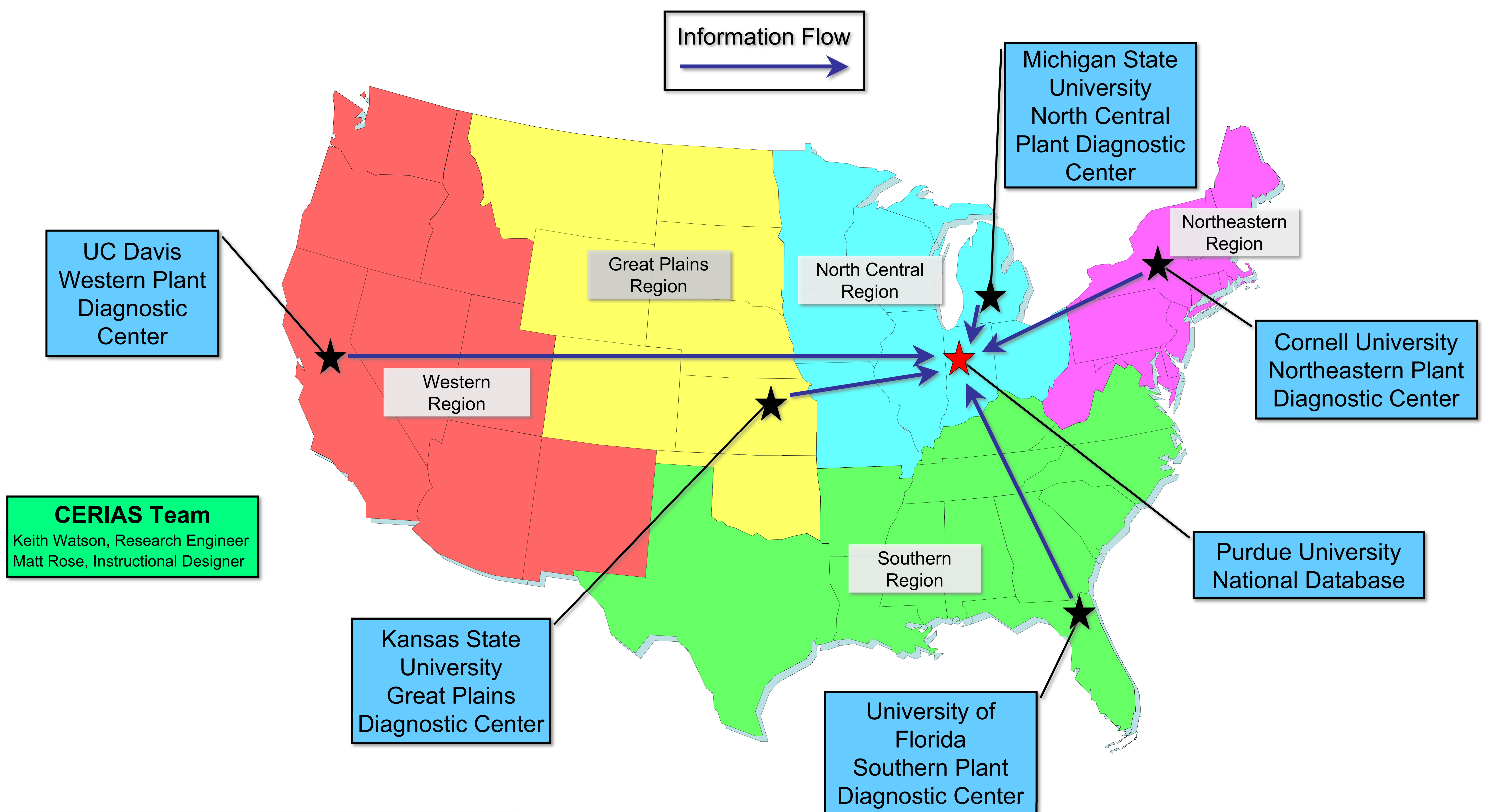


CERIAS

Securing the National Plant Diagnostic Network



National Plant Diagnostic Network

The National Plant Diagnostic Network (NPDN) is a USDA-funded plant biosecurity program. The mission of the Network is to enhance national agricultural security by quickly detecting introduced pests and pathogens. This is achieved through a nationwide network of public agricultural institutions with a cohesive, distributed system to quickly detect deliberately introduced, high consequence, biological pests and pathogens into agricultural and natural ecosystems by providing means for quick identifications and establishing protocols for immediate reporting to appropriate responders and decision makers. The Network will allow land grant university diagnosticians and faculty, state regulatory personnel, and first detectors to efficiently communicate information, images, and methods of detection throughout the system in a timely manner.

CERIAS

CERIAS is assisting the NPDN in developing an effective information security program. Security assessments were conducted at each regional center and the national database facility to identify security issues. Security policy review is underway. Technical training is being developed for the NPDN regional IT personnel, as well as security awareness materials for all personnel associated with the NPDN.



Assessment

Security Assessments for networks, systems, applications, operations, and physical protection. Self-assessments conducted by NPDN staff.

Policy Development

Creation of an information security program and appropriate security policies for the NPDN and the regional centers.

Training

Custom security training for NPDN IT staff. Security Awareness needs analysis and web-based training for all NPDN staff and diagnosticians.

Security Improvement

Improvements made to information systems to protect the confidentiality, integrity, and availability of sensitive NPDN information. Development of security standards, procedures, and business continuity, disaster recovery, and incident response plans.