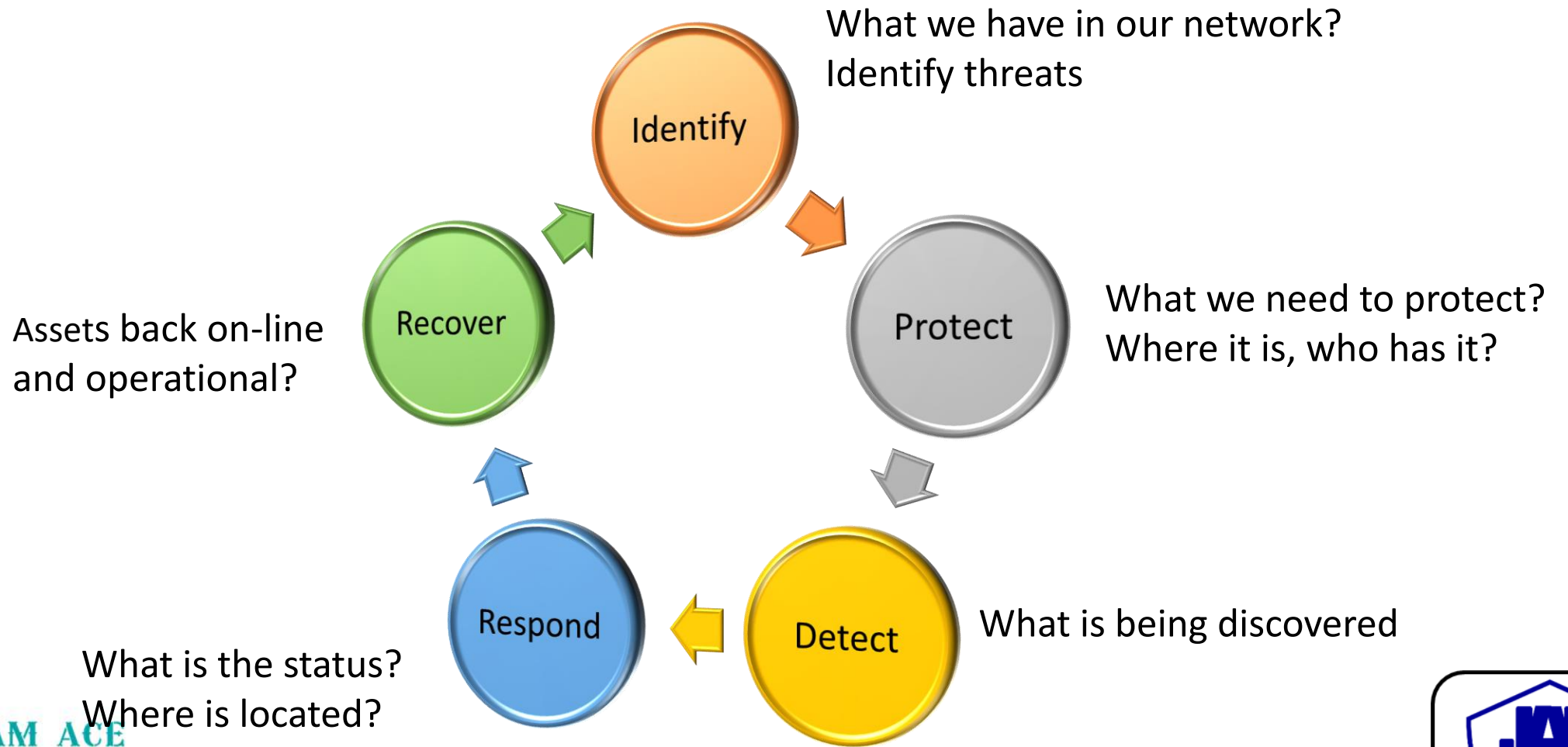# Introduction

- Certified IT Asset Manager (SW, HW, Cloud, Mobil, IoT)
- Over 15 years implementing ITAM programs
- Infrastructure architect, capacity planner
- Project Management, ITIL
- Technical articles writer
- Cybersecurity certified
- Promotes ITAM + Cybersecurity partnership

Cybersecurity Lifecycle - NIST

What we have in our network?
Identify threats

What we need to protect?
Where it is, who has it?

What is being discovered

Assets back on-line
and operational?

What is the status?
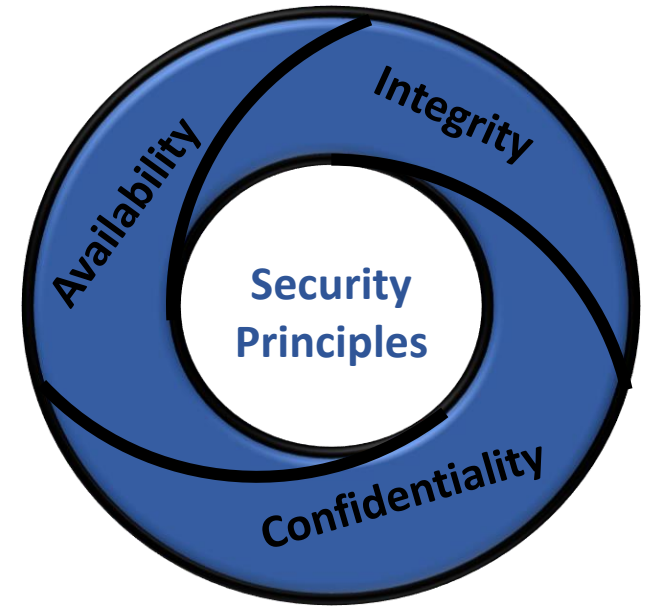Where is located?

Why Cybersecurity + ITAM?

- Availability:
  - Ensures reliability and access to data by authorized individuals
  - More resilient environment by removing vulnerabilities
- Integrity:
  - Ensures accuracy of information
  - Prevents unauthorized modification
- Confidentiality:
  - Ensures secrecy is enforced
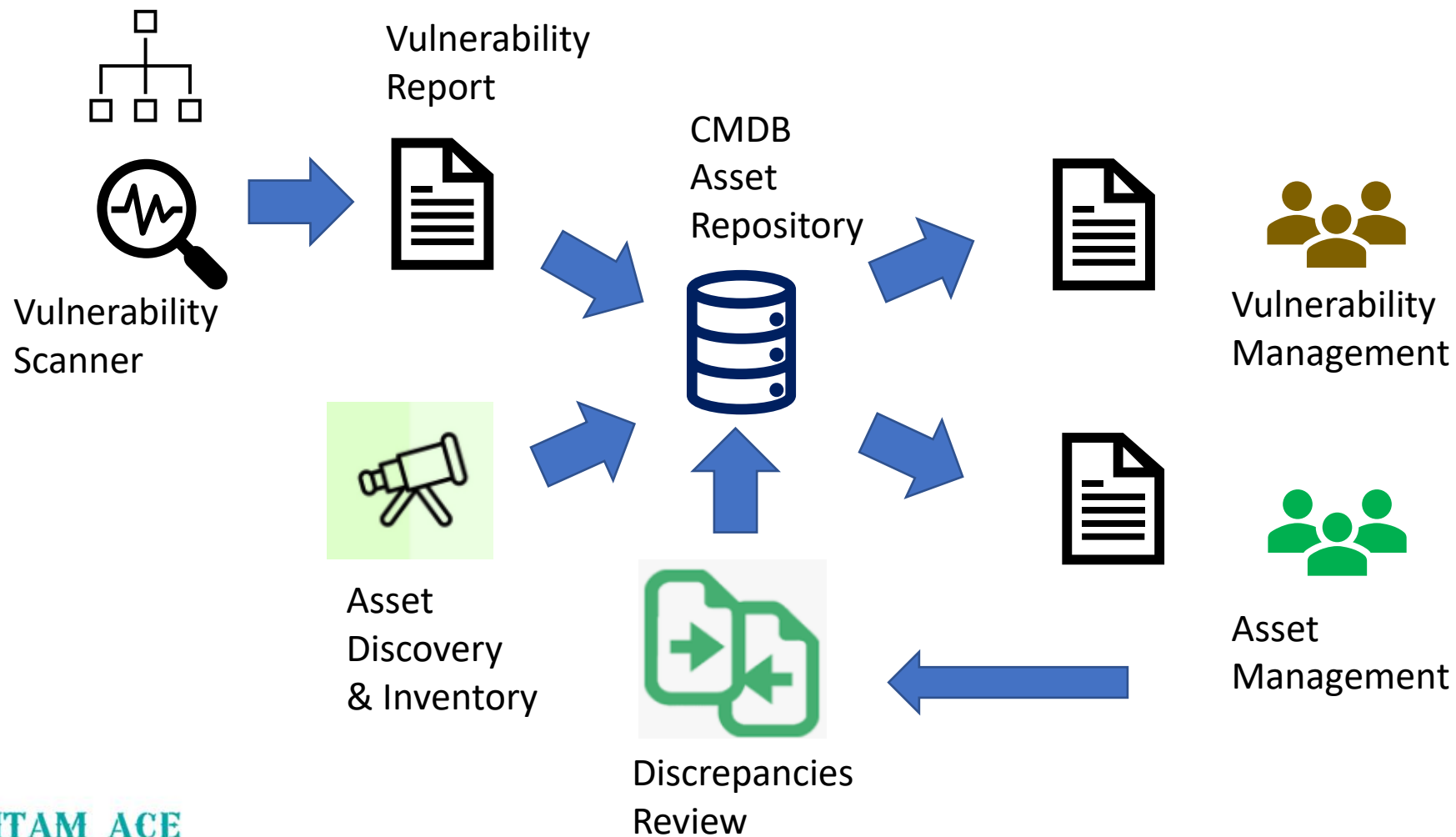 - Prevents unauthorized disclosure

Why IT Asset Management + Cybersecurity?

Plan
Acquire

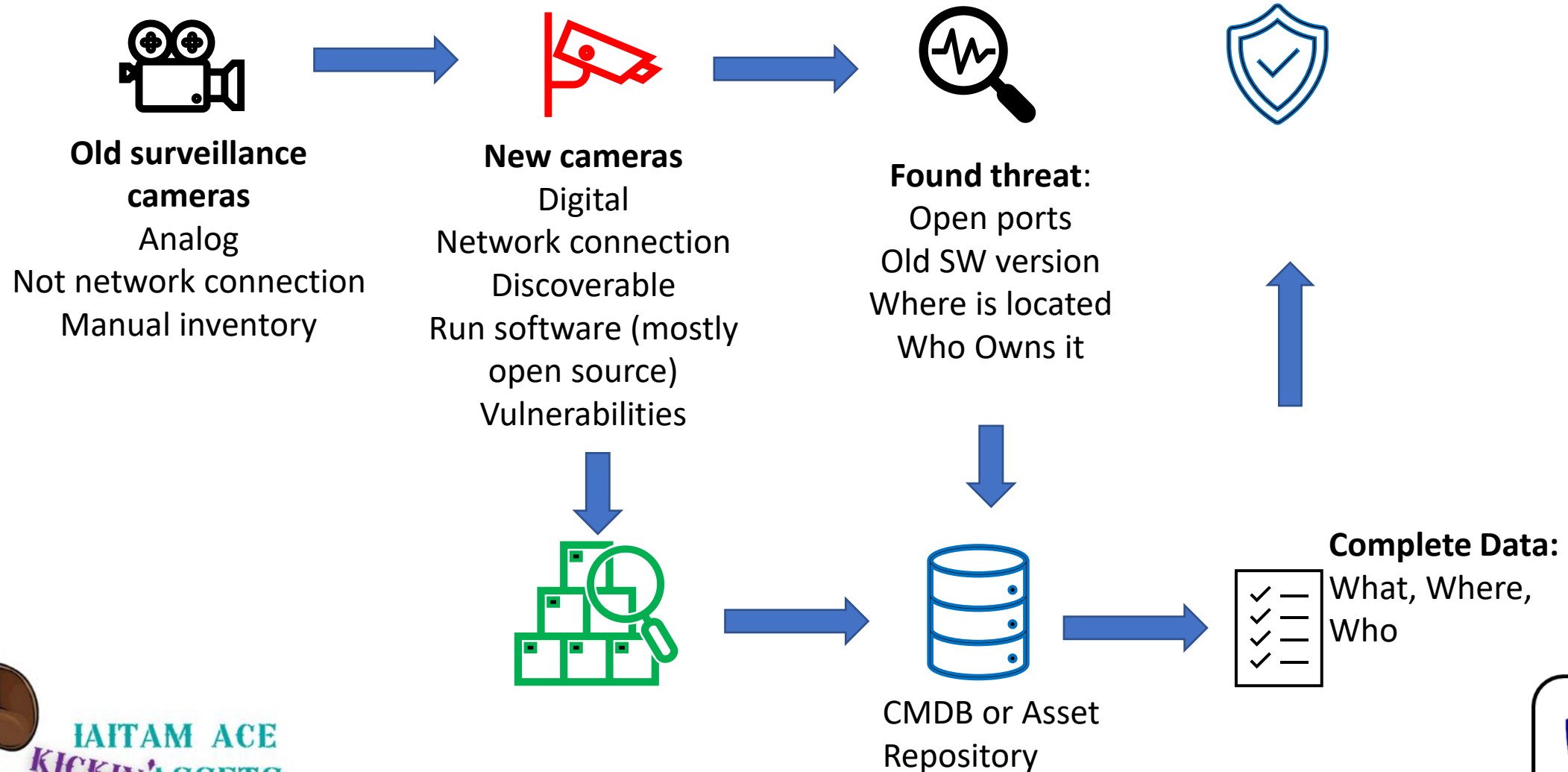Identify
Deploy
Manage

Retire
and
Disposal
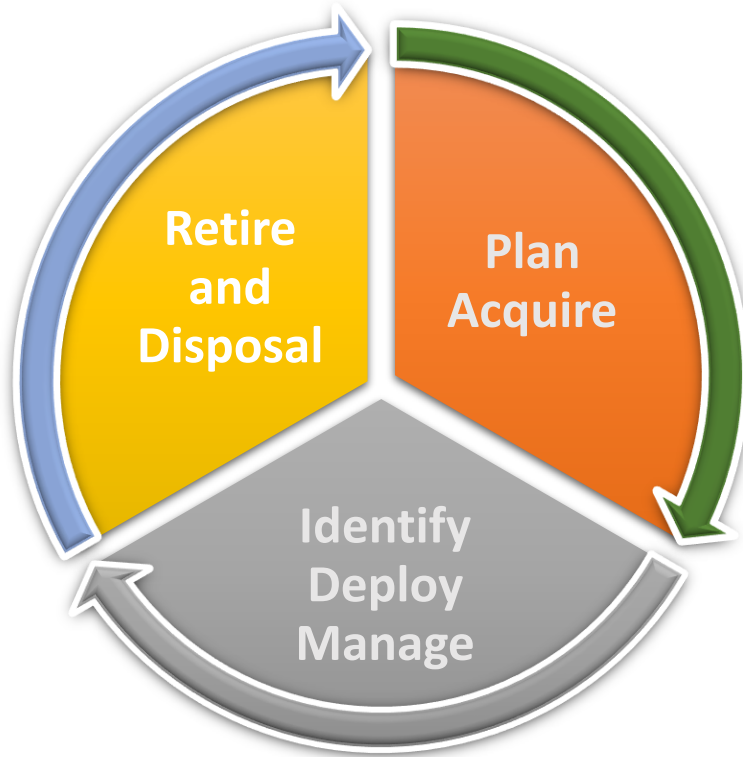
- What, Where, Who for each asset
- Relationship assets with business services (Service Mapping)
- More resilient environment by removing vulnerabilities
- Whitelist, Blacklist, detecting unauthorized software
- Helps with identification of potential risk
- Do we see all that we need to protect?
- Ability to match users to locations
- Reduces blind spots

ITAM + Cybersecurity Collaboration - Vulnerability Management

ITAM + Cybersecurity Collaboration - IoT Devices

Old surveillance cameras
Analog
Not network connection
Manual inventory

New cameras
Digital
Network connection
Discoverable
Run software (mostly open source)
Vulnerabilities

Found threat:
Open ports
Old SW version
Where is located
Who Owns it

Complete Data:
What, Where, Who

CMDB or Asset Repository

IAITAM ACE KICKIN'ASSETS SINCE 2002

Center of Internet Security (CIS) and ITAM

"The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation."

"CIS is an independent, nonprofit organization with a mission to create confidence in the connected world."

CIS Control Related to IT Asset Management

CIS Control 1. Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

CIS Critical Security Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Conclusion

❑ A mature IT Asset Management practice is the foundation of a solid Cybersecurity program

❑ Work under the umbrella of an IT Service Management Framework like ITIL v4.

❑ Collaboration and elimination of silos and barriers is done through defining common goals

❑ ITAM and Cybersecurity must work hand to hand to ensure the success of both practices. There are data and processes to share

CONNECT WITH US

FACEBOOK

TWITTER

INSTAGRAM

IAITAM.org| ACE 2023 | Nashville TN