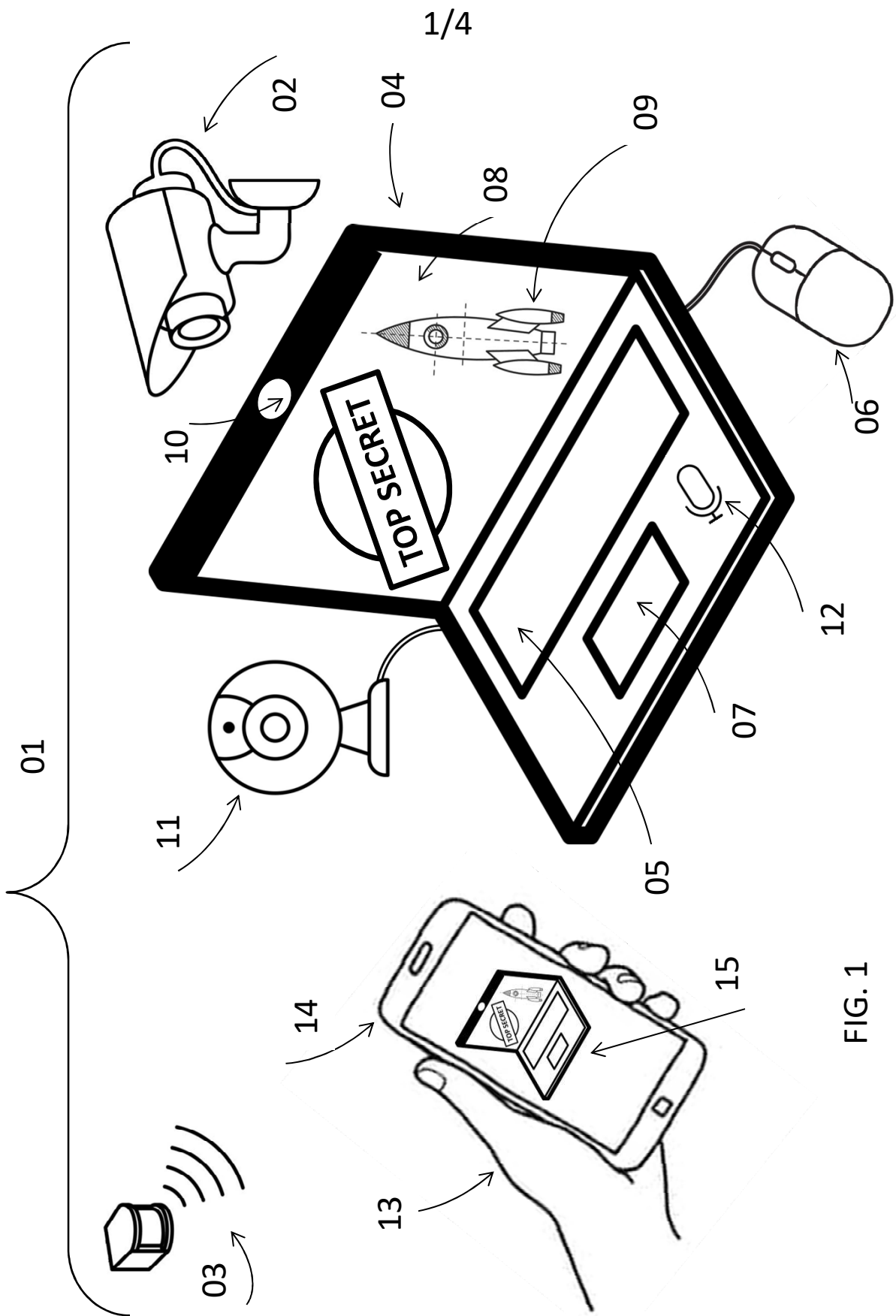




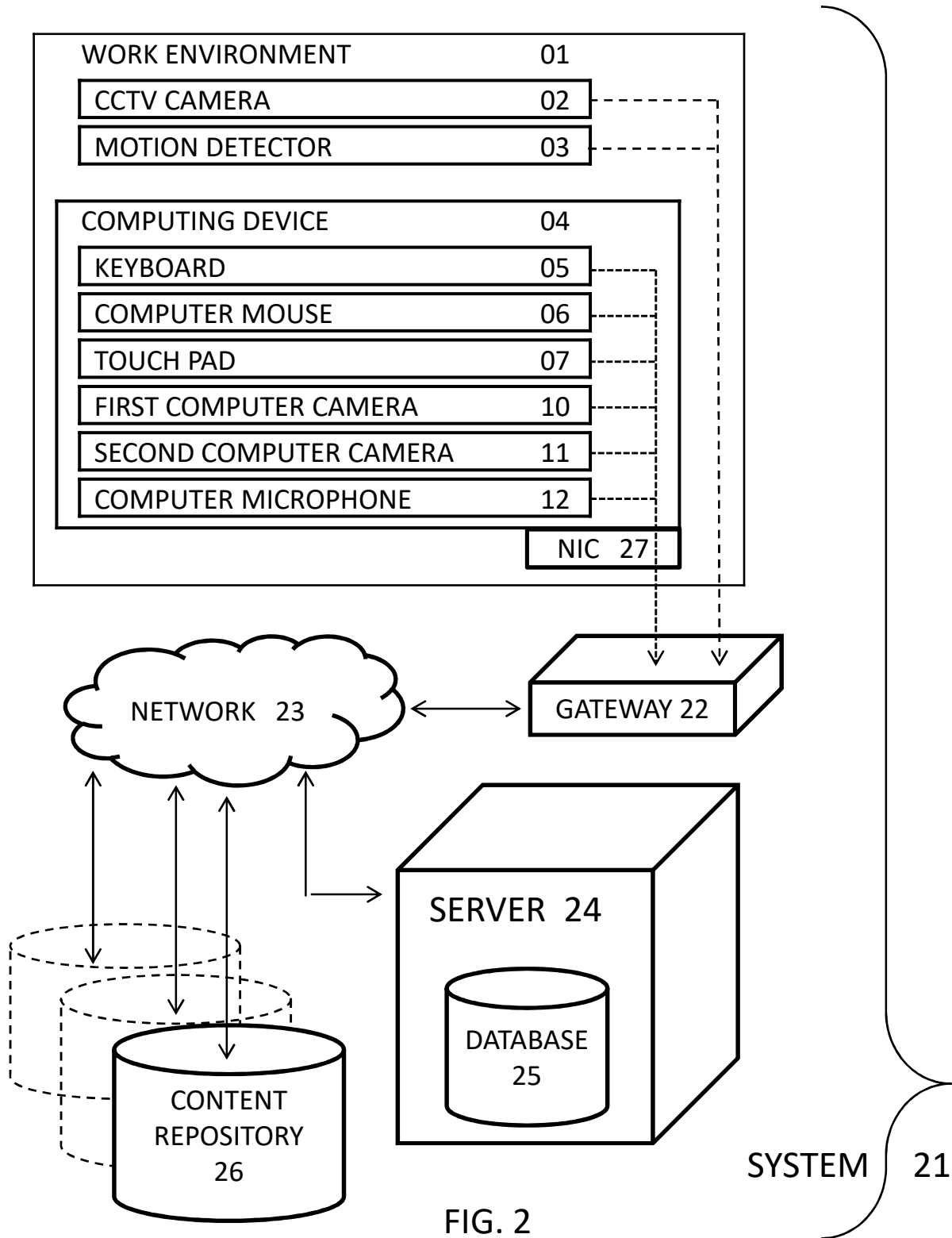


FIG. 2

3/4

3-00



INSTALL SURVEILLANCE SOFTWARE ON THE COMPUTING DEVICES FOR THE WORK ENVIRONMENT TO CAPTURE A STREAM OF IMAGES FOR AT LEAST A PORTION OF THE VIEWING CONE OF THE SECURE MONITOR FROM EACH COMPUTING DEVICE FOR ANALYSIS AS PART OF A SURVEILLANCE FEED	3-01
CONNECT CCTV CAMERAS AND MOTION DETECTORS TO THE GATEWAY AND ROUTE THEIR SUBSTREAMS TO THE SERVER FOR ANALYSIS AS AN ADDITIONAL PART OF THE SURVEILLANCE FEED	3-02
ANALYSE THE STREAM OF IMAGES TO IDENTIFY A CAMERA UNIT THAT IS WITHIN THE VIEWING CONE OF THE SECURE MONITOR AND POSITIONED TO PHOTOGRAPH THE CONTENT DISPLAYED ON THE SECURE MONITOR	3-03
STORE A TRIGGER RECORD WITH A TIME STAMP, A SCREENSHOT OF THE SECURE MONITOR, AND AN IMAGE OF THE POTENTIAL BAD ACTOR	3-04
LOCK DOWN THE COMPUTING DEVICE FOR THE ASSOCIATED SECURE MONITOR THAT ENCOUNTERED THE TRIGGERING EVENT	3-05
SEND A SECURITY ALERT TO A SECURITY PROFESSIONAL	3-06
ATTEMPT TO IDENTIFY AND LOCATE THE POTENTIAL BAD ACTOR BASED ON INFORMATION FROM THE SURVEILLANCE FEED	3-07



FIG. 3

4/4

4-00



EQUIPMENT	STREAM
FIRST COMPUTER CAMERA	FIRST SUBSTREAM OF IMAGES
SECOND COMPUTER CAMERA	SECOND SUBSTREAM OF IMAGES
CCTV CAMERA	THIRD SUBSTREAM OF IMAGES
COMPUTER MICROPHONE	AUDIO
COMPUTER KEYBOARD	TYPING CADENCE
COMPUTER POINTER	POINTER CONTROL CHARACTERISTICS

FIG. 4

5-00



DEACTIVATE THE SECURE MONITOR	5-01
CLOSE ONE OR MORE WINDOWS DISPLAYING THE CONTENT ON THE SECURE MONITOR	5-02
LOCK EACH COMPUTER FILE DISPLAYED ON THE SECURE MONITOR	5-03
DELETE EACH COMPUTER FILE DISPLAYED ON THE SECURE MONITOR FROM THE COMPUTING DEVICE	5-04
RESTRICT ACCESS TO THE COMPUTING DEVICE FOR THE AUTHORIZED USER LOGGED INTO THE COMPUTING DEVICE ASSOCIATED WITH THE SECURE MONITOR DURING THE TRIGGERING EVENT	5-05
RESTRICT ACCESS TO EACH CONTENT REPOSITORY ACCESSIBLE BY THE COMPUTING DEVICE CONNECTED TO THE TRIGGERING EVENT	5-06
WIPE AT LEAST A PORTION OF A LOCAL STORAGE DRIVE OF THE COMPUTING DEVICE ASSOCIATED WITH THE TRIGGERING EVENT	5-07



FIG. 5